ĐẬU THẾ CẤP

Cấu trúc ĐẠI SỐ

$X/Kerf \cong Y$



NHÀ XUẤT BẢN GIÁO DỤC

ĐẬU THẾ CẤP

CẤU TRÚC ĐẠI SỐ

(Tái bản lần thứ ba)

NHÀ XUẤT BẢN GIÁO DỤC

Nhà xuất bản Giáo dục tại TP. Hồ Chí Minh giữ quyền công bố tác phẩm.

Mọi tổ chức, cá nhân muốn sử dụng tác phẩm dưới mọi hình thức phải được sự đồng ý của chủ sở hữu quyền tác giả.

04 – 2009/CXB/399 – 2117/GD Mã số : 7K580m9 – DAI

LỜI NÓI ĐẦU

Quyển sách này được biên soạn trên cơ sở bài giảng Cấu trúc đại số của tác giả tại khoa Giáo dục Tiểu học, Trường Đại học Sư phạm Thành phố Hồ Chí Minh.

Cấu trúc đại số *(phần cơ bản của Đại số đại cương) là một môn học quan trọng của sinh viên khoa Toán các trường Đại học Khoa học Tự nhiên, Đại học Sư phạm và Cao đẳng Sư phạm.*

Môn học Cấu trúc đại số giúp chúng ta hiểu biết lí thuyết tổng quát về phép toán, biết được rằng số tự nhiên, số nguyên, số hữu tỉ, v.v... cùng với các phép toán trên chúng chỉ là các mô hình của những cấu trúc đại số tổng quát. Vì lí do trên, cấu trúc đại số cũng là một môn học quan trọng của sinh viên ngành Giáo dục Tiểu học. Hơn nữa do đặc điểm của chương trình đào tạo Cử nhân Giáo dục Tiểu học, trong sách còn đề cập đến một vài vấn đề của cấu trúc thứ tự.

Sách gồm bốn chương :

1. Phép toán đại số và nửa nhóm.

2. Nhóm.

3. Vành và trường.

4. Một số loại vành đặc biệt.

Cuối mỗi chương của sách có một số bài tập chọn lọc.

Ngoài các bài tập đơn thuần để bạn đọc rèn luyện khả năng vận dụng lí thuyết và phát triển tư duy, trong sách còn có một số bài tập lí thuyết. Khi giải các bài tập lí thuyết, ngoài việc rèn luyện kĩ

năng giải toán bạn đọc còn bổ sung được cho mình về kiến thức của môn học.

Đối tượng phục vụ chính của sách là sinh viên không phải chuyên ngành toán. Do đó các kiến thức chỉ trình bày ở mức độ tổng quát vừa phải. Mặc dù vậy, chúng tôi cho rằng quyển sách nhỏ này cũng rất hữu ích cho sinh viên chuyên ngành toán và đặc biệt là những bạn đọc bước đầu tìm hiểu về môn học thú vị này.

Để quyển sách được hoàn chỉnh hơn khi tái bản, chúng tôi rất mong nhận được nhiều sự góp ý của bạn đọc và của các bạn đồng nghiệp.

TÁC GIẢ

CHƯƠNG I

PHÉP TOÁN ĐẠI SỐ VÀ NỬA NHÓM

§1. ĐỊNH NGHĨA PHÉP TOÁN

1. Định nghĩa và ví dụ

Cho X là một tập hợp. Ta gọi *một phép toán* trên X là một ánh xạ

$$T : X \times X \to X$$

từ tích Decartes $X \times X$ vào X.

Như vậy phép toán T đặt mỗi cặp phần tử (x, y) của tập $X \times X$ với một phần tử duy nhất T(x, y) của X. Phần tử T(x, y) gọi là *kết quả* của phép toán T. Thay cho cách viết T(x, y) ta sẽ viết là xTy và thay cho kí hiệu T ta còn viết các kí hiệu khác như +, ., *, o, ...

x + y được đọc là *x cộng y* và kết quả đó gọi là *tổng* của x và y.

x.y (hay xy) được đọc là *x nhân y* và kết quả đó gọi là *tích* của x và y.

Ví dụ 1. Với phép toán ở vế phải là "phép toán" mà ta đã quen biết thì

a) $T_1(x, y) = x + y$ là phép toán trên $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

b) $T_2(x, y) = x.y$ là phép toán trên $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

c) $T_3(x, y) = x^y$ là phép toán trên $\mathbb{N}^*$.

Ví dụ 2. Kí hiệu X^X là tập các ánh xạ từ X vào chính nó. Khi đó phép hợp thành của hai ánh xạ f, g $\in X^X$

$$T_4(f, g) = g \circ f$$

là phép toán trên X^X.

Ví dụ 3. a) Phép trừ là phép toán trên $\mathbb{Z}$ nhưng không là phép toán trên $\mathbb{N}$.

b) Phép chia là phép toán trên $\mathbb{Q}^*$ nhưng không là phép toán trên $\mathbb{Q}$, không là phép toán trên $\mathbb{Z}^*$.

2. Phép toán cảm sinh

Cho $*$ là một phép toán trên X và A là một tập con của X. Phép toán $*$ gọi là *ổn định trên tập A* nếu với mọi x, y $\in$ A đều có $x * y \in A$.

Nếu phép toán $*$ ổn định trên A thì

$$T : A \times A \rightarrow A, T(x, y) = x * y$$

cũng là một ánh xạ, do đó cũng là một phép toán trên A.

Phép toán này trên tập A được gọi là *phép toán cảm sinh* bởi phép toán $*$ trên X.

Ví dụ 4. a) Phép cộng trên $\mathbb{Z}$ ổn định trên tập con $\mathbb{N}$, ổn định trên tập con $\mathbb{C}$ các số nguyên chẵn. Do đó phép cộng trên $\mathbb{N}$ và $\mathbb{C}$ cảm sinh bởi phép cộng trên $\mathbb{Z}$.

b) Phép trừ trên $\mathbb{Z}$ không ổn định trên tập con $\mathbb{N}$. Do đó phép trừ trên $\mathbb{Z}$ không cảm sinh một phép toán trên $\mathbb{N}$.

Ví dụ 5. Trên $\mathbb{R}$ xét phép toán

$$a \circ b = a + b - ab.$$

Phép toán $\circ$ ổn định trên tập S =[0, 1].

Thật vậy, $a \circ b = a + b - ab = a(1 - b) + b$. Với mọi a, b $\in$ S :

$$0 \le a(1 - b) + b \le (1 - b) + b = 1.$$

Vậy $a \circ b \in S$ với mọi a, b $\in$ S.

§2. CÁC TÍNH CHẤT ĐẶC BIỆT CỦA PHÉP TOÁN

1. Tính chất kết hợp

Cho $*$ là một phép toán trên tập X. Phép toán $*$ gọi là có tính chất *kết hợp* nếu mọi x, y, z $\in$ X ta có

$$(x * y)*z = x*(y * z).$$

Ví dụ 6. a) Phép +, . trên $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ là kết hợp.

b) Phép – trên $\mathbb{Z}$ không kết hợp. Chẳng hạn

$$(1 - 2) - 3 \neq 1 - (2 - 3).$$

c) Phép lũy thừa trên $\mathbb{N}^*$ không kết hợp. Chẳng hạn

$$\left(2^1\right)^2 \neq 2^{\left(1^2\right)}.$$

d) Phép hợp thành các ánh xạ trên X^X là kết hợp.

2. Tính chất giao hoán

Cho $*$ là một phép toán trên tập X. Phép toán $*$ gọi là có tính chất *giao hoán* nếu mọi x, y $\in$ X ta có

$$x * y = y * x.$$

Ví dụ 7. a) Phép +, . trên **N**, **Z**, **Q**, **R** là giao hoán.

b) Phép – trên **Z** không giao hoán. Chẳng hạn

$$1 - 2 \neq 2 - 1.$$

c) Phép lũy thừa trên $\mathbf{N}^*$ không giao hoán. Chẳng hạn

$$1^2 \neq 2^1.$$

d) Nếu X có nhiều hơn một phần tử thì phép toán hợp thành $\circ$ trên X^X không giao hoán. Thật vậy, giả sử a, b $\in$ X, a $\neq$ b.

Gọi f và g $\in X^X$ là các ánh xạ xác định bởi

f(x) = a với mọi x $\in$ X

g(x) = b với mọi x $\in$ X.

Khi đó $g \circ f(a) = b$, $f \circ g(a) = a$. Vậy $g \circ f \neq f \circ g$.

§3. CÁC PHẦN TỬ ĐẶC BIỆT CỦA PHÉP TOÁN

1. Phần tử trung hòa

Cho $*$ là một phép toán trên tập X. Phần tử e' $\in$ X (e'' $\in$ X) gọi là *phần tử trung hòa bên trái (phải)* của phép toán $*$ nếu với mọi x $\in$ X

$$e' * x = x \qquad (x * e'' = x).$$

Phần tử e gọi là *phần tử trung hòa* của phép toán $*$ nếu e vừa là phần tử trung hòa bên trái vừa là phần tử trung hòa bên phải, tức là với mọi $x \in X$

$$e * x = x * e = x.$$

Định lí 1. *Cho $*$ là một phép toán trên X. Khi đó nếu e' là phần tử trung hòa bên trái và e" là phần tử trung hòa bên phải của $*$ thì e' = e".*

CHỨNG MINH. Do e' là phần tử trung hòa bên trái nên

$$e' * e'' = e''.$$

Do e" là phần tử trung hòa bên phải nên

$$e' * e'' = e'.$$

Từ hai đẳng thức trên suy ra e' = e".

Hệ quả. *Phần tử trung hòa của một phép toán $*$, nếu có, là duy nhất.*

Ví dụ 8. a) 0 là phần tử trung hòa của phép cộng trên $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

b) 1 là phần tử trung hòa của phép nhân trên $\mathbb{N}^*$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

c) 0 là phần tử trung hòa bên phải của phép trừ trên $\mathbb{Z}$, nhưng không là phần tử trung hòa bên trái.

d) Ánh xạ đồng nhất I_X là phần tử trung hòa của phép toán $\circ$ trên X^X.

2. Phần tử đối xứng

Cho $*$ là một phép toán trên X có phần tử trung hòa là e. Phần tử $x' \in X$ ($x'' \in X$) gọi là *phần tử đối xứng bên trái (phải)* của x nếu

$$x' * x = e \quad (x * x'' = e).$$

Phần tử x' gọi là *phần tử đối xứng* của x nếu x' vừa là phần tử đối xứng bên phải vừa là phần tử đối xứng bên trái của x, tức là

$$x' * x = x * x' = e.$$

Nếu x có phần tử đối xứng thì x gọi là phần tử khả đối xứng.

Định lí 2. *Nếu phép toán $*$ trên X kết hợp, x' là phần tử đối xứng bên trái của x, x" là phần tử đối xứng bên phải của x thì x' = x".*

CHỨNG MINH. Theo giả thiết ta có

$$\begin{aligned} x' &= x' * e \\ &= x' * (x * x'') \\ &= (x' * x) * x'' \\ &= e * x'' \\ &= x'' \end{aligned}$$

Vậy x' = x".

Hệ quả. *Nếu phép toán kết hợp thì phần tử đối xứng của một phần tử nếu có là duy nhất.*

Ví dụ 9. a) Trên $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ với phép cộng, mọi phần tử x có phần tử đối xứng là $-x$.

b) Trên $\mathbb{Q}^*$, $\mathbb{R}^*$ với phép nhân, mọi phần tử x có phần tử đối xứng là x^{-1}.

c) Trên X^X với phép toán $\circ$, phần tử f khả đối xứng khi và chỉ khi f là song ánh. Phần tử đối xứng của f là ánh xạ ngược f^{-1} của f.

d) Nếu e là phần tử trung hòa của phép toán $*$ trên X thì e khả đối xứng và phần tử đối xứng của e là chính nó.

3. Vài quy ước về cách gọi

Nếu phép toán trên X là phép cộng (+) thì phần tử trung hòa thường gọi là *phần tử không*, kí hiệu là 0_X hoặc 0; phần tử đối xứng của x gọi là *phần tử đối* của x, kí hiệu là $-x$.

Nếu phép toán trên X là phép nhân (.) thì phần tử trung hòa thường gọi là *phần tử đơn vị*, kí hiệu là 1_X hoặc 1; phần tử khả đối xứng gọi là *phần tử khả nghịch*, phần tử đối xứng của x gọi là *phần tử nghịch đảo* của x, kí hiệu là x^{-1}. Cũng như với phép nhân số thông thường dấu (.) thường được bỏ đi.

§4. PHÉP TOÁN n-ngôi

Cho X là một tập hợp và số $n \in \mathbb{N}$. Ta gọi *lũy thừa Descartes bậc n* của X là tập X^n các ánh xạ từ tập rỗng vào X nếu n = 0 và từ tập $\{1, 2, ..., n\}$ vào X nếu n > 0.

Nếu n = 0 thì X^0 có duy nhất một phần tử. Nếu n > 0 thì mỗi phần tử của X^n có thể mô tả dưới dạng một bộ n phần tử $(x_1, x_2, ..., x_n)$, $x_1, x_2, ..., x_n \in X$.

Định nghĩa. *Cho X là một tập hợp và số $n \in \mathbb{N}$. Ta gọi* một phép toán n-ngôi *trên X là một ánh xạ*

$$T : X^n \to X.$$

Theo định nghĩa này, phép toán mà ta xét ở trên là phép toán 2-ngôi.

Khi n = 0, X^0 chỉ có một phần tử, nên phép toán 0-ngôi trên X là một ánh xạ từ tập một phần tử vào X, tức là phép chọn một phần tử của X.

Khi n = 1, $X^1 \equiv X$, do đó phép toán 1-ngôi trên X là một ánh xạ từ X vào X.

Ví dụ 10. $T : \mathbb{N} \to \mathbb{N}, x \mapsto x + 2$ là phép toán 1-ngôi trên X. Đây là phép toán cộng một số tự nhiên với 2.

§5. NỬA NHÓM

1. Định nghĩa nửa nhóm

Cho X là một tập và $*$ là một phép toán trên X. Tập X cùng với phép toán $*$ được kí hiệu là (X, $*$) hoặc X.

(X, $*$) gọi là *một nửa nhóm* nếu phép toán $*$ có tính chất kết hợp.

(X, $*$) gọi là *một vị nhóm* nếu phép toán $*$ kết hợp và có phần tử trung hòa.

Nửa nhóm (vị nhóm) (X, $*$) gọi là *nửa nhóm (vị nhóm) giao hoán* nếu phép toán $*$ là giao hoán.

Ví dụ 11. a) $(\mathbb{N}^*, +)$ là một nửa nhóm giao hoán, nhưng không là vị nhóm; $(\mathbb{N}, +)$ là một vị nhóm.

b) $(\mathbb{N}^*, .)$, $(\mathbb{N}, .)$, $(\mathbb{Z}, .)$ là các vị nhóm giao hoán.

c) (X^X, o) là vị nhóm. Nếu X có nhiều hơn một phần tử thì vị nhóm này không giao hoán.

Ví dụ 12. Cho X là một tập hợp. Trên X xét phép toán

$$x * y = x \text{ với mọi } x, y \in X.$$

• (X, ∗) là một nửa nhóm. Thật vậy, mọi x, y, z ∈ X, ta có : $(x * y) * z = x * z = x$; $x * (y * z) = x * y = x$ nên $(x * y) * z = x * (y * z)$. Vậy phép toán ∗ kết hợp.

• Nếu X có hơn một phần tử thì nửa nhóm (X, ∗) không giao hoán. Thật vậy, giả sử x, y ∈ X, x ≠ y, ta có $x * y = x$, $y * x = y$, tức là $x * y \neq y * x$.

• Mọi y ∈ X đều là phần tử trung hòa bên phải. Thật vậy, mọi x ∈ X ta có $x * y = x$ nên y là phân tử trung hòa bên phải.

• Nếu X có hơn một phần tử thì trong X không có phần tử trung hòa bên trái. Thật vậy, với mọi y ∈ X, chọn x ∈ X, x ≠ y. Khi đó $y * x = y \neq x$ nên y không là phần tử trung hòa bên trái.

2. Tích các phần tử trong nửa nhóm

Cho (X, .) là một nửa nhóm nhân. Vì phép toán kết hợp nên với các phần tử $x_1, x_2, \dots, x_n \in X$ ta định nghĩa.

$$x_1 x_2 x_3 = (x_1 x_2) x_3$$

$$x_1 x_2 \dots x_{n-1} x_n = (x_1 x_2 \dots x_{n-1}) x_n \quad \text{với } n \geq 3.$$

Định lí 3. *Cho $x_1, x_2, \dots, x_n$ là các phần tử của một nửa nhóm X. Giả sử $1 = k_1 < k_2 < \dots < k_h \leq n$. Đặt*

$$b_1 = a_1 a_2 \dots a_{k_2 - 1}$$

$$b_2 = a_{k_2} a_{k_2+1} \dots a_{k_3 - 1}$$

....

$$b_h = a_{k_h} a_{k_h+1} \dots a_n.$$

Khi đó ta có $a_1 a_2 \dots a_n = b_1 b_2 \dots b_h$.

CHỨNG MINH. Hiển nhiên kết quả đúng với $n \le 3$. Giả sử kết quả đúng với $n - 1 \ge 3$, ta sẽ chứng minh kết quả đúng với n.

• Nếu $k_h = n$ thì $b_h = a_n$. Theo giả thiết quy nạp

$$a_1 a_2 ... a_{n-1} = b_1 b_2 ... b_{k_h - 1},$$

suy ra
$$a_1 a_2 ... a_{n-1} . a_n = b_1 b_2 ... b_{k_h - 1} b_h .$$

• Nếu $k_h < n$ thì ta đặt $b'_{k_h} = a_{k_h} a_{k_h + 1} ... a_{n-1}$.

Theo giả thiết quy nạp

$$a_1 a_2 ... a_{n-1} = (b_1 b_2 ... b_{k_h - 1}) b'_{k_h},$$

suy ra
$$a_1 a_2 ... a_{n-1} a_n = (b_1 b_2 ... b_{k_h - 1})(b'_{k_h} a_n)$$
$$= (b_1 b_2 ... b_{k_h - 1}) b_{k_h}$$
$$= b_1 b_2 ... b_{k_h} .$$

Nhận xét 1. 1) Ta viết a a ... a (n lần) là a^n. Theo định lí 3, với mọi phần tử a của nửa nhóm nhân X và $p, q \in \mathbf{N}^*$ ta có

$$a^p a^q = a^{p+q}$$
$$a^{pq} = (a^p)^q$$

2) Nếu X là nửa nhóm cộng thì ta viết a + a + ... + a (n lần) là n a. Các quy tắc trong 1) trở thành : Với mọi $a \in X$, $p, q \in \mathbf{N}^*$ ta có

$$pa + qa = (p + q)a$$
$$(pq) a = q(pa).$$

Định lí 4. *Cho $x_1, x_2, \ldots, x_n$ là các phần tử của một nửa nhóm giao hoán X. Khi đó*

$$x_1 x_2 \ldots x_n = x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)}$$

trong đó σ là một hoán vị bất kì của các số 1, 2,..., n.

CHỨNG MINH. Hiển nhiên kết quả đúng với $n \le 3$. Giả sử kết quả đúng với $n - 1 \ge 3$, ta sẽ chứng minh kết quả đúng với n. Với hoán vị σ bất kì, đặt $\sigma(n) = k$. Ta có

$$\begin{aligned} a_1 a_2 \ldots a_n &= (a_1 \ldots a_{k-1}) a_k (a_{k+1} \ldots a_n) \text{ (theo định lí 1)} \\ &= (a_1 \ldots a_{k-1})(a_{k+1} \ldots a_n) a_k \\ &= (a_1 \ldots a_{k-1} a_{k+1} \ldots a_n) a_k \\ &= (a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n-1)}) a_{\sigma(n)} \text{ (do giả thiết quy nạp)} \\ &= a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n-1)} a_{\sigma(n)}. \end{aligned}$$

Nhận xét 2. 1) Theo định lí 4, với mọi $a, b \in X$, X là nửa nhóm giao hoán và $n \in \mathbb{N}^*$ ta có

$$(ab)^n = a^n b^n.$$

2) Nếu X là nửa nhóm cộng giao hoán thì quy tắc trong 1) trở thành $n(a + b) = na + nb$.

3. Tính chất của phần tử khả nghịch

Định lí 5. *Cho X là một vị nhóm với phần tử đơn vị 1_X. Khi đó*

1) $1_X^{-1} = 1_X$.

2) $x \in X$ khả nghịch thì x^{-1} khả nghịch và $(x^{-1})^{-1} = x$.

3) $x, y \in X$ khả nghịch thì xy khả nghịch và $(xy)^{-1} = y^{-1}x^{-1}$.

CHỨNG MINH.

1) Vì $1_X 1_X = 1_X$.

2) Vì $x x^{-1} = x^{-1} x = 1_X$.

3) Vì $(y^{-1} x^{-1})(xy) = y^{-1} 1_X y = y^{-1} y = 1_X$,

$(xy)(y^{-1} x^{-1}) = x \; 1_X x^{-1} = x x^{-1} = 1_X$.

Nhận xét 4. Nếu (X, +) là một vị nhóm với phần tử không 0_X thì các quy tắc trong định lí 5 trở thành

1) $-0_X = 0_X$.

2) $-(-x) = x$ nếu x có phần tử đối.

3) $-(x + y) = -y - x$ nếu x, y có phần tử đối.

Ở đây ta sử dụng kí hiệu $x + (-y) = x - y$, đọc là x trừ y, nếu y có phần tử đối.

4. Luật giản ước

Phần tử a của nửa nhóm nhân X gọi là *thỏa mãn luật giản ước* nếu mọi x, y ∈ X, ta có

$$ax = ay \text{ suy ra } x = y,$$

$$xa = ya \text{ suy ra } x = y.$$

Định lí 6. *Nếu a là phần tử khả nghịch của một vị nhóm X thì a thỏa mãn luật giản ước.*

CHỨNG MINH. Với mọi x, y ∈ X ta có

$$ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay)$$

$$\Rightarrow (a^{-1}a)x = (a^{-1}a)y$$

$$\Rightarrow 1_X x = 1_X y$$

$$\Rightarrow x = y.$$

Tương tự ta cũng có

$$xa = ya \Rightarrow x = y.$$

§6. NỬA NHÓM CON

Cho (X, ∗) là một nửa nhóm và tập con $A \subset X$ ổn định đối với phép toán ∗. Phép toán ∗ cảm sinh trên A hiển nhiên là kết hợp, do đó (A, ∗) là một nửa nhóm, gọi là *nửa nhóm con* của (X, ∗).

Để chứng minh A là một nửa nhóm con của X ta chỉ cần kiểm tra phép toán trên X là ổn định trên A.

Nếu X là vị nhóm và nửa nhóm con A của X chứa phần tử trung hòa của X thì A là một vị nhóm và được gọi là vị nhóm con của X.

Ví dụ 13. Trong tập $\mathbb{Z}$ xét C là tập con các số chẵn và L là tập con các số lẻ. Khi đó C là vị nhóm con của vị nhóm ($\mathbb{Z}$, +), L là vị nhóm con của vị nhóm ($\mathbb{Z}$, .).

Ví dụ 14. Xét tập **R** với phép toán

$$a \circ b = a + b - ab$$

và tập con S = [0, 1]. Với mọi $a, b, c \in \mathbf{R}$ ta có

$$\begin{aligned}(a \circ b) \circ c &= (a + b - ab) \circ c \\ &= a + b - ab + c - c(a + b - ab) \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

Tương tự ta tính được $a \circ (b \circ c)$ và có $(a \circ b) \circ c = a \circ (b \circ c)$.

Vì phép toán $\circ$ kết hợp nên $(\mathbb{R}, \circ)$ là một nửa nhóm.

Mọi a, b $\in \mathbb{R}$, ta có $a \circ b = a + b - ab = b + a - ba = b \circ a$ nên phép toán $\circ$ giao hoán.

Mọi a $\in \mathbb{R}$, ta có $a \circ 0 = a + 0 - a.0 = a$, $0 \circ a = a$.

Do đó 0 là phần tử trung hòa của phép toán $\circ$.

Vậy $(\mathbb{R}, \circ)$ là một vị nhóm giao hoán. Theo ví dụ 5, S là nửa nhóm con của $(\mathbb{R}, \circ)$. Do $0 \in S$ nên S là vị nhóm con của $(\mathbb{R}, \circ)$.

Ví dụ 15. Nếu X là nửa nhóm thì X là một nửa nhóm con của X. Nếu X là một vị nhóm thì X và $\{1_X\}$ là vị nhóm con của X.

§7. ĐỒNG CẤU NỬA NHÓM

Cho hai nửa nhóm $(X, *)$ và $(Y, \circ)$. Một ánh xạ

$$f : X \to Y$$

gọi là một *đồng cấu nửa nhóm* nếu

$$f(x * y) = f(x) \circ f(y) \text{ với mọi } x, y \in X.$$

Nếu X và Y đều là vị nhóm thì đồng cấu nửa nhóm gọi là *đồng cấu vị nhóm*.

Khi ánh xạ f là đơn ánh, toàn ánh, song ánh thì đồng cấu f tương ứng được gọi là *đơn cấu, toàn cấu, đẳng cấu.*

Ví dụ 16. Cho $f : (\mathbb{N}, +) \to (\mathbb{N}, .)$, $f(n) = 2^n$

Ta có $f(m + n) = 2^{m+n} = 2^m.2^n = f(m).f(n)$ với mọi m, n $\in \mathbb{N}$, nên f là đồng cấu. Dễ thấy f là đơn ánh nên f là đơn cấu từ $(\mathbb{N}, +)$ vào $(\mathbb{N}, .)$. Chú ý rằng f cũng là đơn cấu vị nhóm.

Ví dụ 17. a) Cho X là một nửa nhóm (vị nhóm). Khi đó ánh xạ đồng nhất

$$I_X : X \to X, I_X(x) = x \text{ với mọi } x \in X$$

là đẳng cấu nửa nhóm (vị nhóm).

b) Cho A là một nửa nhóm con của X. Khi đó ánh xạ

$$j_A : A \to X,\ j_A(x) = x \text{ với mọi } x \in A$$

là đơn cấu nửa nhóm, gọi là phép nhúng chính tắc A vào X.

c) Cho X là một nửa nhóm, Y là một vị nhóm. Khi đó ánh xạ

$$f : X \to Y,\ f(x) = 1_Y \text{ với mọi } x \in X$$

là đồng cấu nửa nhóm. Đặc biệt, nếu X là vị nhóm thì ánh xạ $f : X \to X$, $f(x) = 1_X$ với mọi $x \in X$ là đồng cấu vị nhóm.

Định lí 7. *Cho $f : (X, *) \to (Y, \circ)$ là một đồng cấu nửa nhóm. Khi đó*

1) A là nửa nhóm con của X thì f(A) là nửa nhóm con của Y.

2) B là nửa nhóm con của Y thì $f^{-1}(B)$ là nửa nhóm con của X.

CHỨNG MINH. 1) Lấy tùy ý $y_1, y_2 \in f(A)$. Khi đó tồn tại x_1, $x_2 \in A$ sao cho $f(x_1) = y_1$, $f(x_2) = y_2$. Từ đó

$$y_1 \circ y_2 = f(x_1) \circ f(x_2) = f(x_1 * x_2)$$

Vì $x_1 * x_2 \in A$ nên $y_1 \circ y_2 \in f(A)$. Vậy f(A) là nửa nhóm con của Y.

2) Lấy tùy ý $x_1, x_2 \in f^{-1}(B)$. Khi đó $f(x_1), f(x_2) \in B$. Do B là nửa nhóm nên $f(x_1) \circ f(x_2) = f(x_1 * x_2) \in B$. Suy ra $x_1 * x_2 \in f^{-1}(B)$. Vậy $f^{-1}(B)$ là nửa nhóm con của X.

Ví dụ 18. Theo ví dụ 16 ta có $f(\mathbb{N}) = \{2^n \mid n \in \mathbb{N}\}$ là nửa nhóm con của nhóm $(\mathbb{N}, .)$.

§8. NỬA NHÓM SẮP THỨ TỰ

1. Nửa nhóm sắp thứ tự

Cho $(X, *)$ là một nửa nhóm giao hoán và $\leq$ là một quan hệ thứ tự toàn phần trên X. Nếu mọi $x, y, z \in X$

$$x \leq y \Rightarrow x * z \leq y * z \qquad (1)$$

thì $(X, *, \leq)$ gọi là *một nửa nhóm sắp thứ tự.*

Nếu $x \leq y$ và $x \neq y$ thì ta viết $x < y$. Nếu điều kiện (1) thay bởi điều kiện

$$x < y \Rightarrow x * z < y * z$$

thì nửa nhóm gọi là *nửa nhóm sắp thứ tự nghiêm ngặt.*

Trên $\mathbb{N}$ hoặc $\mathbb{Z}$ ta có quan hệ thứ tự thông thường :

$m \leq n$ nếu tồn tại $k \in \mathbb{N}$ sao cho $m + k = n$.

Ta có $\leq$ là quan hệ thứ tự toàn phần trên $\mathbb{N}$ và trên $\mathbb{Z}$.

Ví dụ 19. a) $(\mathbb{N}, +, \leq)$, $(\mathbb{N}^*, ., \leq)$ là nửa nhóm sắp thứ tự nghiêm ngặt; $(\mathbb{N}, ., \leq)$ là nửa nhóm sắp thứ tự (không nghiêm ngặt)

b) $(\mathbb{Z}, +, \leq)$ là nửa nhóm sắp thứ tự nghiêm ngặt; $(\mathbb{Z}, ., \leq)$ không là nửa nhóm sắp thứ tự.

c) Mọi nửa nhóm con của một nửa nhóm sắp thứ tự là nửa nhóm sắp thứ tự.

2. Đồng cấu đơn điệu

Cho $(X, \leq)$ và $(Y, \leq)$ là hai tập được sắp. Một ánh xạ $f : X \to Y$ gọi là *đơn điệu* nếu mọi $x, y \in X$

$$x \leq y \Rightarrow f(x) \leq f(y). \qquad (2)$$

Nếu điều kiện (2) được thay bởi

$$x < y \Rightarrow f(x) < f(y)$$

thì f được gọi là *đơn điệu nghiêm ngặt*.

Một đồng cấu gọi là *đồng cấu đơn điệu* hay *đơn điệu nghiêm ngặt* nếu ánh xạ f có tính chất đó.

Ví dụ 20. $f : (\mathbb{N}, +) \to (\mathbb{N}, +)$, $f(n) = 2n$ với mọi $n \in \mathbb{N}$ là đồng cấu đơn điệu nghiêm ngặt.

3. Nửa nhóm sắp thứ tự Archimedes

Cho nửa nhóm sắp thứ tự nghiêm ngặt $(X, *, \leq)$. Phần tử $a \in X$ gọi là *phần tử dương* nếu $x < a * x$ với mọi $x \in X$.

Nửa nhóm sắp thứ tự nghiêm ngặt $(X, *, \leq)$ gọi là *sắp thứ tự Archimedes* nếu mọi $a, b \in X$, b là phần tử dương, đều tồn tại $n \in \mathbb{N}$ sao cho

$$a < b * b * \ldots * b \text{ (n lần)}$$

Nếu X là nửa nhóm cộng thì điều kiện trên được viết lại là $a < nb$.

Ví dụ 21. a) Trong $(\mathbb{N}, +)$ và $(\mathbb{Z}, +)$ phần tử dương là mọi $a \in \mathbb{N}^*$. Trong $(\mathbb{N}, .)$ phần tử dương là $a \neq 0$, $a \neq 1$.

b) $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}, .)$ là nửa nhóm sắp thứ tự Archimedes.

BÀI TẬP CHƯƠNG I

1.1. Xét các tính chất và phần tử đặc biệt của các phép toán :

a) $m * n = m + 2n$ trên $\mathbb{N}$;

b) $m * n = m.2^n$ trên $\mathbb{N}$.

c) $m * n = m + n^2$ trên $\mathbb{Z}$.

1.2. Trên $\mathbb{N}^*$ đặt :

a) $a * b$ = ƯCLN (a, b),

b) $a \odot b$ = BCNN $[a, b]$.

$*$ và $\odot$ có là phép toán trên $\mathbb{N}$ không ? Nếu là phép toán hãy xét các tính chất và các phần tử đặc biệt.

1.3. Trên $\mathbb{N}^*$ với phép toán $m * n = m^n$. Chứng minh rằng

a) $(m * n) * p = m * (n * p) \Leftrightarrow m = 1$ hoặc $p = 1$ hoặc $n = 2, p = 2$.

b) Nếu $m \neq n$ thì $m * n = n * m \Leftrightarrow m = 2, n = 4$.

1.4. Cho $*$ là một phép toán trên X. Chứng minh rằng tập con

$$S = \{x \in X \mid (x * y) * z = x * (y * z) \text{ với mọi } x, y \in X\}$$

ổn định với phép toán trên X và $(S, *)$ là một nửa nhóm.

1.5. Chứng minh rằng các tập và các phép toán tương ứng sau đây là những nửa nhóm giao hoán.

a) $\mathbb{R}$, $x * y = x + y + xy$.

b) $\mathbb{N}$, $x \oplus y = x + y + 2$.

1.6. Trên $\mathbb{R}^*$ xét phép toán $a * b = |a|b$. Chứng tỏ $(\mathbb{R}^*, *)$ là một nửa nhóm không giao hoán.

1.7. Phép toán $*$ trên X gọi là lũy đẳng nếu $x * x = x$ với mọi x. Cho $(X, *)$ là một nửa nhóm giao hoán lũy đẳng. Trên X đặt

$$x \leq y \text{ nếu } x * y = y.$$

Chứng minh $\leq$ là một quan hệ thứ tự trên X.

1.8. Kí hiệu $\mathscr{P}(X)$ là tập tất cả các tập con của X.

a) Chứng tỏ $(\mathscr{P}(X), \cup)$ là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

b) Chứng tỏ $(\mathscr{P}(X), \cap)$ là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

1.9. Trên tập $S = [0, 1]$ đặt $a * b = \min\{a + b, 1\}$. Chứng tỏ $(S, *)$ là một vị nhóm giao hoán. Tìm các phần tử khả đối xứng của vị nhóm này.

1.10. Cho X là một nửa nhóm và $a, b \in X$ là hai phần tử thỏa mãn $ab = ba$. Chứng minh rằng $(ab)^n = a^n b^n$ với mọi $n \in \mathbb{N}^*$.

1.11. Trong nửa nhóm X^X các ánh xạ từ tập X vào tập X với phép toán hợp thành của ánh xạ, chứng minh rằng

a) f thỏa mãn luật giản ước trái (tức $f \circ g = f \circ h \Rightarrow g = h$) $\Leftrightarrow$ f là đơn ánh.

b) f thỏa mãn luật giản ước phải (tức $g \circ f = h \circ f \Rightarrow g = h$) $\Leftrightarrow$ f là toàn ánh.

c) f thỏa mãn luật giản ước $\Leftrightarrow$ f là song ánh.

CHƯƠNG II

NHÓM

§1. ĐỊNH NGHĨA VÀ TÍNH CHẤT

1. Định nghĩa nhóm

Một vị nhóm được gọi là *một nhóm* nếu mọi phần tử của nó đều khả đối xứng.

Nếu phép toán của nhóm giao hoán thì nhóm được gọi là *nhóm giao hoán* hay *nhóm Abel*.

Như vậy nhóm có thể được định nghĩa trực tiếp như sau :

• *Tập X cùng với một phép toán nhân trên nó gọi là một nhóm nếu thỏa mãn các điều kiện sau*

(G_1) Mọi $x, y, z \in X$

$$(xy)z = x(yz)$$

(G_2) Tồn tại $1_X \in X$ (gọi là phần tử đơn vị) sao cho với mọi $x \in X$

$$1_X x = x 1_X = x$$

(G_3) Mọi $x \in X$ tồn tại $x^{-1} \in X$ (gọi là phần tử nghịch đảo của x) sao cho

$$x^{-1}x = xx^{-1} = 1_X.$$

• *Tập X cùng với một phép toán cộng trên nó gọi là một nhóm nếu thỏa mãn các điều kiện sau*

(G_1) *Mọi* $x, y, z \in X$

$$(x + y) + z = x + (y + z)$$

(G_2) *Tồn tại* $0_X \in X$ *(gọi là phần tử không) sao cho với mọi* $x \in X$

$$0_X + x = x + 0_X = x$$

(G_3) *Mọi* $x \in X$ *tồn tại* $-x \in X$ *(gọi là phần tử đối của x) sao cho*

$$(-x) + x = x + (-x) = 0_X.$$

Nhận xét 1. Trong một nhóm nhân có phép chia (:) được định nghĩa như sau : $x : y = xy^{-1}$.

Trong một nhóm cộng có phép trừ (–) được định nghĩa như sau: $x - y = x + (-y)$.

2) Thông thường, phép cộng được sử dụng khi nhóm là giao hoán, còn phép nhân được sử dụng cho cả nhóm giao hoán và không giao hoán. Để đơn giản kí hiệu, các kết quả lí thuyết về sau ta thường chỉ xét với nhóm nhân. Tương tự như trong chương I, dễ dàng chuyển các kết quả này cho nhóm cộng hay nhóm với phép toán tùy ý.

3) Theo định nghĩa thì một nửa nhóm có thể là tập rỗng, còn nhóm bao giờ cũng chứa ít nhất một phần tử, đó là phần tử trung hòa.

Ví dụ 1. a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ là nhóm Abel. Phần tử không là 0, phần tử đối của x là $-x$.

b) $(\mathbb{Q}^*, .)$, $(\mathbb{Q}^*_+, .)$ là nhóm Abel. Phần tử đơn vị là 1, phần tử nghịch đảo của x là $\frac{1}{x}$.

c) Tập S_X các song ánh từ X lên chính nó với phép hợp thành ánh xạ (tích ánh xạ) là một nhóm. Phần tử đơn vị của S_X là I_X, phần tử nghịch đảo của f là f^{-1}, ánh xạ ngược của f. Nếu X có nhiều hơn hai phần tử thì S_X không giao hoán. Nếu X = {1, 2, ..., n} thì S_X được kí hiệu là S_n và gọi là *nhóm các phép thế bậc n*.

Ví dụ 2. Với mỗi $k \in \mathbb{N}^*$ cố định ta định nghĩa quan hệ S trên $\mathbb{Z}$

$$x \, S \, y \text{ nếu } x - y \; \vdots \; k.$$

Dễ dàng kiểm tra S là quan hệ tương đương trên $\mathbb{Z}$. Kí hiệu tập thương của $\mathbb{Z}$ theo quan hệ S là $\mathbb{Z}_k$. Ta có

$$\mathbb{Z}_k = \{\overline{0}, \overline{1}, \ldots, \overline{k-1}\},$$

trong đó $\overline{j} = \{x \in \mathbb{Z} \mid x - j \; \vdots \; k\}$, gọi là lớp đồng dư với j theo môđun k.

Trên $\mathbb{Z}_k$ ta định nghĩa phép cộng và nhân như sau

$\overline{m} + \overline{n} = \overline{r}$, r là số dư trong phép chia m + n cho k.

$\overline{m}.\overline{n} = \overline{s}$, s là số dư trong phép chia m.n cho k

Dễ dàng kiểm tra rằng : $(\mathbb{Z}_k, +)$ là một nhóm Abel, phần tử không là $\overline{0}$, phần tử đối của $\overline{m}$ là $\overline{k-m}$; $(\mathbb{Z}_k, .)$ là một vị nhóm giao hoán với phần tử đơn vị là $\overline{1}$.

Ta kí hiệu $\mathbb{Z}_k^* = \mathbb{Z}_k \setminus \{\overline{0}\}$.

Có thể chứng minh rằng nếu k > 1 thì $(\mathbb{Z}_k^*, .)$ là nhóm khi và chỉ khi k là số nguyên tố. Chẳng hạn $(\mathbb{Z}_4^*, .)$ không là nhóm vì phần tử $\overline{2}$ không có phần tử nghịch đảo ($\overline{2}.\overline{j} \neq \overline{1}$ với mọi j = 1, 2, 3).

Với mọi $\overline{m}, \overline{n}, \overline{p} \in \mathbb{Z}_k$ ta còn có $\overline{m}(\overline{n} + \overline{p}) = \overline{m}\,\overline{n} + \overline{m}\,\overline{p}$.

2. Tính chất của các phần tử trong nhóm

Nếu a là phần tử của một nhóm X thì ta định nghĩa

$$a^o = 1$$

$$a^n = a\,a \ldots a \ (n \text{ lần}) \quad \text{nếu } n > 0$$

$$a^n = (a^{-1})^{|n|} \qquad \text{nếu } n < 0.$$

Theo nhận xét 1 và 2 chương I, suy ra :

1) Với mọi phần tử a của một nhóm X và p, q $\in \mathbb{Z}$ ta có

$$a^p . a^q = a^{p+q}$$

$$a^{pq} = (a^p)^q .$$

2) Với mọi phần tử a, b của một nhóm X và m $\in \mathbb{Z}$ ta có

$$(a.b)^m = a^m b^m .$$

Theo định lí 5 chương I suy ra :

3) Với mọi phần tử a, b của một nhóm X ta có

$$(a^{-1})^{-1} = a, \ (ab)^{-1} = b^{-1}a^{-1} .$$

Theo định lí 6 chương I suy ra :

4) Mọi phần tử của một nhóm X đều thỏa mãn luật giản ước, tức là mọi a, b, c $\in$ X

$$ab = ac \Rightarrow b = c; \ ba = ca \Rightarrow b = c.$$

§2. NHÓM CON

1. Định nghĩa nhóm con

Cho X là một nhóm và tập con A của X ổn định với phép toán trên X. Nếu A cùng với phép toán cảm sinh là một nhóm thì A gọi là *nhóm con* của X.

Một cách tương đương, nhóm con có thể định nghĩa như sau :

Tập con A của nhóm X gọi là một nhóm con của X nếu thỏa mãn ba điều kiện sau đây :

1) Mọi $x, y \in A$ đều có $xy \in A$;

2) $1_X \in A$;

3) Mọi $x \in A$ đều có $x^{-1} \in A$.

Thật vậy, nếu A thỏa mãn ba điều kiện trên thì với phép toán cảm sinh A là một nhóm, do đó A là nhóm con của X. Ngược lại nếu A là nhóm con của X thì do A ổn định với phép toán trên X nên có 1°). Gọi 1_A là phần tử đơn vị của nhóm A thì $1_A.1_X = 1_A.1_A$, vì 1_A thỏa mãn luật giản ước nên $1_X = 1_A \in A$, tức là có 2°). Với mọi $x \in A$ ký hiệu x_A^{-1} là nghịch đảo của x trong A. Khi đó $x.x^{-1} = x.x_A^{-1}\left(= 1_X\right)$, vì x thỏa mãn luật giản ước nên $x^{-1} = x_A^{-1} \in A$, tức là cũng có 3°).

Nhận xét 2. 1) Nếu A là nhóm con của nhóm X thì đơn vị của A cũng chính là đơn vị của X; nghịch đảo của $x \in A$ trong A cũng chính là nghịch đảo của x trong X.

2) Nếu A là nhóm con của một vị nhóm X (tức là với phép toán cảm sinh A là một nhóm) thì điều nói trên có thể không đúng. Chẳng hạn : ($\mathbb{Z}$,.) là một vị nhóm, $A = \{0\} \subset \mathbb{Z}$ hiển nhiên là một nhóm con của ($\mathbb{Z}$,.). Đơn vị của A là 0 khác đơn vị của ($\mathbb{Z}$,.) là 1, nghịch đảo của 0 trong A là 0 còn 0 không khả nghịch trong ($\mathbb{Z}$,.).

Ví dụ 3. a) Tập con các số nguyên chẵn là nhóm con của nhóm ($\mathbb{Z}$,+).

b) $\mathbf{Q}^*_+$ là nhóm con của nhóm ($\mathbf{Q}^*$,.).

c) $\{-1,1\}$ là nhóm con của nhóm ($\mathbf{R}^*$,.).

d) Với mọi nhóm X, các tập $\{1_X\}$ và X là nhóm con của X. Các nhóm con này gọi là các *nhóm con tầm thường* của X.

2. Các tiêu chuẩn của nhóm con

Định lí 1. *Tập con A của nhóm X là một nhóm con của X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \varnothing$

2) $x, y \in A \Rightarrow xy \in A$

3) $x \in A \Rightarrow x^{-1} \in A$.

CHỨNG MINH. Hiển nhiên $2^o/ \Rightarrow 1)$ nên từ $1^o/$, $2^o/$, $3^o/$ suy ra 1), 2), 3).

Ngược lại, nếu có 1), 2), 3) thì do 1) tồn tại $x \in A$, do 2) tồn tại $x^{-1} \in A$, từ đó do 3) $1_X = x.x^{-1} \in A$, tức là có $2^o/$. Vậy từ 1), 2), 3) suy ra $1^o/$, $2^o/$, $3^o/$.

Định lí 2. *Tập con A của nhóm X là một nhóm con của X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow xy^{-1} \in A$.

CHỨNG MINH. Hiển nhiên $2°/ \Rightarrow 1)$. Với mọi x, y ∈ A theo 3°/ $x, y^{-1} \in A$, theo 2°/ $xy^{-1} \in A$, do đó có 2). Vậy từ 1°/,2°/,3°/ suy ra 1), 2).

Ngược lại, nếu có 1), 2) thì theo 1) tồn tại x ∈ A, theo 2) $1_X = xx^{-1} \in A$, tức là 2°/. Với mọi x ∈ A theo 2) $x^{-1} = 1_X x^{-1} \in A$, tức là có 3°/. Với mọi x, y ∈ A ta có x, $y^{-1} \in A$, từ đó theo 2) $xy = x(y^{-1})^{-1} \in A$, tức là có 1°/. Vậy từ 1), 2) suy ra 1°/, 2°/, 3°/.

3. Nhóm con sinh bởi một tập

Cho S là một tập con của nhóm X. Ta gọi *nhóm con của X sinh bởi tập S* là nhóm con nhỏ nhất chứa tập S, kí hiệu là [S]. Như vậy nhóm con [S] sinh bởi tập S có hai tính chất đặc trưng :

1°/ [S] là nhóm con của X;

2°/ Nếu A là nhóm con của X và $A \supset S$ thì $A \supset [S]$.

Định lí 3. *Mọi tập con S của nhóm X tồn tại và duy nhất nhóm con [S] sinh bởi tập S.*

CHỨNG MINH. Gọi $\mathscr{B}$ là họ tất cả các nhóm con của X chứa S. Vì $X \in \mathscr{B}$ nên $\mathscr{B} \neq \emptyset$. Ta sẽ chứng minh

$$[S] = \bigcap_{B \in \mathscr{B}} B.$$

Theo định nghĩa ta chỉ cần chứng minh $A = \bigcap_{B \in \mathscr{B}} B$ là một nhóm con. Thật vậy, $1_X \in B$ với mọi $B \in \mathscr{B}$ nên $1_X \in A$. Nếu x, y ∈ A thì x,

$y \in B$ với mọi $B \in \mathscr{B}$. Do B là nhóm nên $xy^{-1} \in B$ với mọi $B \in \mathscr{B}$. Vậy $xy^{-1} \in A$. Theo định lí 2, A là nhóm con của X.

Nhận xét 3. $[\emptyset] = 1_X$.

Cho A là một nhóm con của X. Tập con S của X sao cho [S] = A gọi là *tập sinh* của nhóm A.

Hiển nhiên [A] = A nên tập sinh của một nhóm luôn tồn tại. Một nhóm có thể có nhiều tập sinh khác nhau.

Ví dụ 4. Nhóm con $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\}$ ($k \in \mathbb{Z}$ cố định) của $(\mathbb{Z},+)$ sinh bởi tập một phần tử {k}.

Thật vậy, kí hiệu [k] là nhóm con của $\mathbb{Z}$ sinh bởi tập một phần tử k. Khi đó ta có $k \in [k]$ và do đó $-k \in [k]$. Từ đó tổng một số tùy ý của các phần tử $\pm k$ cũng thuộc [k], tức $kn \in [k]$ với mọi $n \in \mathbb{Z}$. Suy ra $k\mathbb{Z} \subset [k]$. Vì $k\mathbb{Z}$ cũng là nhóm con chứa k nên $k\mathbb{Z} = [k]$.

4. Nhóm con cyclic

Cho X là một nhóm. Với mọi $a \in X$ ta gọi nhóm con [a] sinh bởi phần tử a là *nhóm con cyclic* của X. Nếu tồn tại $a \in X$ sao cho X = [a] thì X gọi là *nhóm Cyclic*.

Định lí 4. *Nhóm con cyclic [a] của nhóm X là tập tất cả các phần tử của X có dạng a^m, $m \in \mathbb{Z}$.*

CHỨNG MINH. Đặt $B = \{a^m \mid m \in \mathbb{Z}\}$, ta chứng minh [a] = B. Vì $a, a^{-1} \in [a]$ nên $a^m \in [a]$ với mọi $m \in \mathbb{Z}$, tức là $B \subset [a]$. Mặt khác $a \in B$ và mọi $a^m, a^n \in B$ ta có

$$a^m.(a^n)^{-1} = a^m.a^{-n} = a^{m-n} \in B$$

nên B là nhóm con chứa a, suy ra $B \supset [a]$. Vậy B = [a].

Hệ quả. *Mọi nhóm con cyclic đều là nhóm Abel.*

CHỨNG MINH. Theo định lí 4, mọi phần tử của nhóm cyclic đều có dạng a^m. Ta có $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$ nên nhóm là nhóm Abel.

Định lí 5. *Với mọi nhóm con cyclic $A = [a]$ có một và chỉ một trong hai khả năng sau đây :*

1) Tồn tại $n > 0$ sao cho A có đúng n phần tử và

$$A = \{a^0, a^1, \ldots, a^{n-1}\}$$

2) A có vô hạn phần tử và

$$A = \{a^m \mid m \in \mathbb{Z}\}, \text{ trong đó } a^p \neq a^q \text{ với mọi } p \neq q.$$

CHỨNG MINH. Nếu 2) không xảy ra thì tồn tại $p > q$ sao cho $a^p = a^q$, $a^{p-q} = 1_X$ với $p - q > 0$. Gọi n là số nguyên dương nhỏ nhất để $a^n = 1_X$. Ta sẽ chứng minh $A = \{a^0, a^1, \ldots, a^{n-1}\}$. Với mọi $m \in \mathbb{Z}$ ta viết

$$m = nk + r, \quad 0 \le r \le n - 1.$$

Khi đó $a^m = a^{nk+r} = (a^n)^k . a^r = 1_X a^r = a^r$.

Vậy A chỉ chứa các phần tử $a^0, a^1, \ldots, a^{n-1}$. Với mọi $r_1, r_2, 0 \le r_1 < r_2 \le n - 1$, do n là số dương nhỏ nhất để $a^n = 1_X$, ta có $a^{r_2 - r_1} \neq 1_X$, suy ra $a^{r_1} \neq a^{r_2}$. Vậy A là tập có đúng n phần tử, $A = \{a^0, a^1, \ldots, a^{n-1}\}$.

Ta gọi *cấp* của một nhóm X là số phần tử của X nếu X có hữu hạn phần tử. Trường hợp X có vô hạn phần tử thì ta nói X có *cấp vô hạn*.

Ta gọi *Cấp của phần tử* a của nhóm X là cấp của nhóm con [a].

Ví dụ 5. a) $(\mathbb{Z},+)$ là nhóm cyclic cấp vô hạn vì $\mathbb{Z} = [1]$ hoặc $\mathbb{Z} = [-1]$.

b) $(\mathbb{Z}_6,+)$ là nhóm cyclic cấp 6 (sinh bởi $\overline{1}$), phần tử $\overline{2}$ có cấp 3, phần tử $\overline{3}$ có cấp 2.

§3. NHÓM CON CHUẨN TẮC. NHÓM THƯƠNG

1. Lớp ghép của một nhóm theo một nhóm con

Cho X là một nhóm và A là một nhóm con của X.

Trên X xét quan hệ xS_ty nếu $x^{-1}y \in A$.

- *S_t là một quan hệ tương đương trên X.*

Thật vậy, mọi $x \in X$, $x^{-1}x = 1_X \in A$ nên xS_tx vậy S_t có tính chất phản xạ. Mọi $x, y \in X$ nếu xS_ty thì $x^{-1}y \in A$, suy ra $y^{-1}x = (x^{-1}y)^{-1} \in A$ nên yS_tx vậy S_t có tính chất đối xứng. Mọi $x, y, z \in X$ nếu xS_ty và yS_tz thì $x^{-1}y$ và $y^{-1}z \in A$, từ đó $x^{-1}z = (x^{-1}y)(y^{-1}z) \in A$ nên xS_tz, vậy S_t có tính chất bắc cầu.

Lớp tương đương của X theo quan hệ tương đương S_t chứa x là

$$\{y \in X \mid x^{-1}y \in A\} = \{y \mid x^{-1}y = a, a \in A\}$$

$$= \{y = xa \mid a \in A\}.$$

Ta gọi $xA = \{xa \mid a \in A\}$ là *lớp ghép trái* của x theo nhóm con A. Khi đó lớp tương đương chứa x theo quan hệ tương đương S_t chính là xA.

Tương tự, quan hệ xS_py nếu $yx^{-1} \in A$ cũng là quan hệ tương đương trên X. Lớp tương đương chứa x theo quan hệ tương đương S_p là

$$Ax = \{ax \mid a \in A\}$$

gọi là *lớp ghép phải* của x theo nhóm con A.

Chú ý rằng nếu X là nhóm cộng thì lớp ghép trái và phải theo nhóm con A sẽ là

$$x + A = \{x + a \mid a \in A\}$$

$$A + x = \{a + x \mid a \in A\}.$$

Hiển nhiên rằng $1_X A = A1_X$. Nếu nhóm không giao hoán thì nói chung $xA \neq Ax$.

2. Nhóm con chuẩn tắc

Nhóm con A của nhóm X gọi là *nhóm con chuẩn tắc* nếu $xA = Ax$ với mọi $x \in X$.

Nếu A là nhóm con chuẩn tắc của X thì ta kí hiệu $A \lhd X$.

Ví dụ 6. a) $E = \{1_X\}$ và X là các nhóm con chuẩn tắc của nhóm X.

b) Nếu X là nhóm Abel thì mọi nhóm con của X đều là nhóm con chuẩn tắc.

Định lí 6. *Nhóm con A của nhóm X là nhóm con chuẩn tắc khi và chỉ khi với mọi $x \in X$ và $a \in A$ đều có $xax^{-1} \in A$.*

CHỨNG MINH. Nếu $A \lhd X$ thì mọi $x \in X$, $xA = Ax$. Mọi $a \in A$ thì $xa \in Ax$, do đó tồn tại $b \in A$ để $xa = bx \Rightarrow xax^{-1} = b \in A$.

Ngược lại, với mọi $x \in X$, $a \in A$, $xax^{-1} \in A \Rightarrow xa \in Ax$ với mọi $a \in A \Rightarrow xA \subset Ax$. Ta cũng có $x^{-1}a(x^{-1})^{-1} \in A \Rightarrow x^{-1}ax \in A \Rightarrow ax \in xA$ với mọi $a \in A \Rightarrow Ax \subset xA$. Vậy $xA = Ax$ hay $A \lhd X$.

Nếu $A \lhd X$ thì $xS_t y \Leftrightarrow x^{-1}y \in A \Leftrightarrow x(x^{-1}y)x^{-1} \in A \Leftrightarrow yx^{-1} \in A \Leftrightarrow xS_p y$. Ta kí hiệu chung hai quan hệ S_t và S_p là $x \equiv y$ (mod A) và gọi là quan hệ đồng dư theo môđun A.

Ví dụ 7. Với mọi $m > 0$, $m\mathbb{Z} \lhd (\mathbb{Z}, +)$. Do đó

$$x \equiv y \pmod{m\mathbb{Z}}$$

$$\Leftrightarrow x - y \in m\mathbb{Z}$$

$$\Leftrightarrow x - y \;\vdots\; m$$

$$\Leftrightarrow x \equiv y \pmod{m}.$$

Như vậy quan hệ đồng dư theo môđun $m\mathbb{Z}$ chính là quan hệ đồng dư theo môđun m quen biết.

3. Nhóm thương

Cho A là một nhóm con chuẩn tắc của X. Ta kí hiệu

$$X/A = \{xA \mid x \in X\} = \{Ax \mid x \in X\}$$

là *tập thương* của X theo quan hệ đồng dư môđun A. Ta cũng gọi X/A là *tập thương của X theo nhóm con chuẩn tắc A.*

Trên X/A ta định nghĩa

$$xA.yA = (xy)A.$$

Nếu $xA = x'A$, $yA = y'A$ thì $x^{-1}x' = a \in A$, $y^{-1}y' = b \in A$.

Từ đó $(xy)^{-1}(x'y') = y^{-1}(x^{-1}x')y' = y^{-1}ay'$

$$= (y^{-1}ay)y^{-1}y' = (y'ay)b \in A.$$

Vậy $(xy)A = (x'y')A$, nghĩa là định nghĩa trên xác định một phép toán nhân trên X/A.

Định lí 7. *$(X/A, .)$ là một nhóm.*

CHỨNG MINH. Hiển nhiên mọi xA, yA, zA $\in X/A$ ta có (xA.yA).(zA) = xA.(yA.zA) vì cùng bằng (xyz)A. Vậy phép toán là kết hợp.

Với mọi $xA \in X/A$, $1_X A \,.\, xA = xA \,.\, 1_X A = xA$ nên $1_X A$ là phần tử đơn vị.

Với mọi $xA \in X/A$, $x^{-1}A . xA = xA . x^{-1}A = 1_X A$ nên $x^{-1}A$ là nghịch đảo của xA.

Nhóm X/A gọi là *nhóm thương của nhóm X theo nhóm con chuẩn tắc A.*

Ví dụ 8. Với mọi m > 1, $m\mathbb{Z}$ là nhóm con chuẩn tắc của $(\mathbb{Z}, +)$. Các phần tử của $\mathbb{Z}/m\mathbb{Z}$ có dạng $x + m\mathbb{Z}$, là tập các số nguyên đồng dư với x theo môđun m, ký hiệu là $\overline{x}$. Phép toán $(x + m\mathbb{Z}) + (y + m\mathbb{Z}) = (x + y) + m\mathbb{Z}$ trong $\mathbb{Z}/m\mathbb{Z}$ cũng chính là phép toán cộng của các lớp đồng dư theo môđun m :

$$\overline{x} + \overline{y} = \overline{x + y}.$$

4. Định lí Lagrange

Định lí 8. *Nếu X là một nhóm hữu hạn thì mọi nhóm con A của X cũng hữu hạn và cấp của nhóm con A là ước số của cấp của nhóm X.*

CHỨNG MINH. Xét lớp ghép trái xA của X. Vì ánh xạ $\varphi : A \to xA$, $\varphi(a) = xa$ là một song ánh từ A lên xA nên mọi lớp ghép trái đều có số phần tử bằng cấp của A. Gọi $x_1A, x_2A, \ldots, x_kA$ là các lớp ghép trái khác nhau của X. Khi đó $X = \bigcup_{i=1}^{k} x_iA$, $x_iA \cap x_jA = \varnothing$ với mọi $i \neq j$. Từ đó cấp của nhóm X bằng k lần cấp của nhóm con A.

Nhận xét 4. Cho X là nhóm cấp n, A là nhóm con chuẩn tắc cấp m, X/A có cấp k. Theo định lí Lagrange ta có

$$n : m = k.$$

§4. ĐỒNG CẤU NHÓM

1. Định nghĩa và tính chất

Cho X và Y là hai nhóm, để đơn giản kí hiệu ta đều xét phép toán trên chúng là phép nhân, chú ý rằng phép toán trên X và Y nói chung là khác nhau.

Một ánh xạ $f : X \to Y$ gọi là *một đồng cấu nhóm* nếu mọi $x, y \in X$ đều có $f(x.y) = f(x).f(y)$.

Định lí 9. *Cho $f : X \to Y$ là một đồng cấu nhóm. Khi đó*

1) $f(1_X) = 1_Y$.

2) Với mọi $x \in X$, $f(x^{-1}) = [f(x)]^{-1}$.

CHỨNG MINH. a) Vì $1_X.1_X = 1_X$ nên $f(1_X).f(1_X) = f(1_X)$. Theo luật giản ước ta có $f(1_X) = 1_Y$.

b) Mọi $x \in X$, $xx^{-1} = 1_X$ nên $f(x)\, f(x^{-1}) = f(1_X) = 1_Y$.

Do phần tử khả nghịch của f(x) là duy nhất nên

$$f(x^{-1}) = [f(x)]^{-1}.$$

Khi ánh xạ $f : X \to Y$ là đơn ánh, toàn ánh, song ánh thì đồng cấu f được gọi tương ứng là *đơn cấu, toàn cấu, đẳng cấu.*

Đồng cấu f từ nhóm X vào chính nó được gọi là *tự đẳng cấu.*

Ví dụ 9. a) $\mathbb{Z}$ là nhóm cộng các số nguyên, X là một nhóm nhân bất kì và $a \in X$ là một phần tử cố định. Ánh xạ $f : \mathbb{Z} \to X$, $f(m) = a^m$ là một đồng cấu nhóm.

b) Ánh xạ $f : (\mathbb{R},+) \to (\mathbb{R}^*_+,.)$, $f(x) = 2^x$ là một đẳng cấu nhóm.

c) Cho X và Y là hai nhóm. Ánh xạ $x \mapsto 1_Y$ với mọi $x \in X$ là một đồng cấu nhóm từ X vào Y. Đồng cấu này gọi là đồng cấu tầm thường từ X vào Y.

d) Cho X là một nhóm. Ánh xạ đồng nhất $1_X : X \to X$ là đẳng cấu nhóm.

e) Cho A là một nhóm con của nhóm X. Ánh xa $j_A : A \to X$, $j_A(x) = x$ là đơn cấu nhóm, gọi là phép nhúng chính tắc A vào X.

f) Cho X là một nhóm và A là một nhóm con chuẩn tắc của X. Ánh xa $p : X \to X/A$, $p(x) = xA$ là một toàn cấu, gọi là *toàn cấu chính tắc* X lên X/A.

Định lí 10. *Cho $f: X \to Y$, $g : Y \to Z$ là các đồng cấu nhóm. Khi đó $h : X \to Z$, $h = gof$ là đồng cấu nhóm.*

CHỨNG MINH. Với mọi $x, y \in X$ ta có

$$h(x.y) = g(f(x.y)) = g(f(x)f(y))$$

$$= g(f(x)).\ g(f(y)) = h(x).h(y),$$ do đó h là đồng cấu.

Định lí 11. *Nếu $f : X \to Y$ là một đẳng cấu thì ánh xạ ngược $f^{-1} : Y \to X$ cũng là đẳng cấu.*

CHỨNG MINH. Vì f là song ánh nên ánh xạ ngược f^{-1} tồn tại và cũng là một song ánh. Với mọi x', y' ∈ Y tồn tại duy nhất x, y ∈ X để f(x) = x', f(y) = y'. Từ đó

$$f^{-1}(x'y') = f^{-1}(f(x)\, f(y))$$

$$= f^{-1}(f(xy))$$

$$= I_X(xy)$$

$$= xy$$

$$= f^{-1}(x')\, f^{-1}(y').$$

Vậy f^{-1} là đồng cấu và do đó là đẳng cấu.

2. Ảnh và hạt nhân của đồng cấu.

Định lí 12. *Cho $h : X \to Y$ là một đồng cấu nhóm. Khi đó*

1) A là nhóm con của X thì f(A) là nhóm con của Y.

2) B là nhóm con của Y thì $f^{-1}(B)$ là nhóm con của X.

CHỨNG MINH. 1) Lấy tùy ý y_1, y_2 ∈ f(A). Khi đó tồn tại x_1, x_2 ∈ A sao cho $f(x_1) = y_1$, $f(x_2) = y_2$. Từ đó

$$y_1 y_2^{-1} = f(x_1) \left(f(x_2)\right)^{-1} = f(x_1)\, f\left(x_2^{-1}\right) = f\left(x_1 x_2^{-1}\right).$$

Do $x_1x_2^{-1} \in A$ nên $y_1 y_2^{-1} \in f(A)$. Mặt khác $1_Y = f(1_X) \in f(A)$ nên f(A) là nhóm con của Y.

2) Lấy tùy ý x_1, $x_2 \in f^{-1}(B)$. Khi đó $f(x_1)$, $f(x_2)$ ∈ B.

Do B là nửa nhóm nên $f(x_1).(f(x_2))^{-1} = f(x_1).f\left(x_2^{-1}\right) =$ $= f\left(x_1.x_2^{-1}\right) \in B$. Từ đó suy ra $x_1x_2^{-1} \in f^{-1}(B)$. Hiển nhiên $1_X \in f^{-1}(B)$ nên $f^{-1}(B)$ là nhóm con của X.

Cho $f : X \to Y$ là một đồng cấu nhóm. Theo định lí 12, f(X) là một nhóm con của Y, ta gọi nhóm con này là *ảnh* của f, kí hiệu là Im f ; $f^{-1}(\{1_Y\}) = f^{-1}(1_Y)$ là một nhóm con của X, ta gọi nhóm con này là *hạt nhân* của f, kí hiệu là Ker f.

Định lí 13. *Cho $f : X \to Y$ là một đồng cấu nhóm. Khi đó*

1) Ker f là một nhóm con chuẩn tắc của X.

2) f là đơn cấu khi và chỉ khi Ker f = $\{1_X\}$.

CHỨNG MINH. 1) Lấy tùy ý $x \in X$ và $a \in$ Ker f. Ta có $f(xax^{-1})$ $= f(x)\ f(a)\ f(x^{-1}) = f(x)\ 1_Y (f(x))^{-1} = 1_Y$. Từ đó $xax^{-1} \in$ Ker f. Vậy Ker f $\lhd$ X.

2) Giả sử f là đơn cấu. Với mọi $a \in$ Ker f ta có

$$f(a) = 1_Y = f(1_X) \Rightarrow a = 1_X. \text{ Từ đó Ker } f = \{1_X\}.$$

Ngược lại, giả sử Ker f = $\{1_X\}$. Với mọi $x,y \in X$, $f(x) = f(y)$

$\Rightarrow f(x)\ .\ (f(y))^{-1} = 1_Y \Rightarrow f\left(x.y^{-1}\right) = 1_Y \Rightarrow xy^{-1} \in$ Ker f

$\Rightarrow xy^{-1} = 1_X \Rightarrow x = y$. Vậy f là đơn ánh.

3. Định lí đồng cấu nhóm

Định lí 14. *Cho $f : X \to Y$ là một đồng cấu nhóm, $p : X \to X/_{Ker\ f}$ là toàn cấu chính tắc từ nhóm X lên nhóm thương $X/_{Ker\ f}$. Khi đó tồn tại duy nhất đơn cấu $\bar{f} : X/_{Ker\ f} \to Y$ sao cho $\bar{f} \circ p = f$.*

CHỨNG MINH. Sự tồn tại : Đặt A = Ker f. Ta sẽ chỉ ra $\bar{f} : X/_A \to Y$, $\bar{f}(xA) = f(x)$ có các tính chất đòi hỏi.

Thật vậy, hiển nhiên $\bar{f}$ là ánh xạ. Với mọi xA, yA $\in X/_A$ ta có

$$\bar{f}(xA.yA) = \bar{f}(xyA) = f(xy) = f(x)\,f(y) = \bar{f}(xA).\bar{f}(yA)$$

nên $\bar{f}$ là đồng cấu. Giả sử xA, yA $\in X/_A$, $xA \neq yA \Rightarrow x^{-1}y \notin A$

$$\Rightarrow f(x^{-1}y) \neq 1_Y \Rightarrow (f(x))^{-1} f(y) \neq 1_Y \Rightarrow f(x) \neq f(y)$$

$\Rightarrow \bar{f}(xA) \neq \bar{f}(yA)$. Vậy $\bar{f}$ là đơn cấu.

Cuối cùng, với mọi $x \in X$ ta có $\bar{f}_o\, p(x) = \bar{f}(xA) = f(x)$ nên $\bar{f}_o\, p = f$.

Tính duy nhất : Nếu $\bar{f}' : X/_A \to Y$ cũng có tính chất đòi hỏi thì $\bar{f}'{}_o p = f$. Từ đó với mọi xA$\in X/_A$ ta có

$$\bar{f}'(xA) = \bar{f}'(p(x)) = f(x) = \bar{f}(xA).$$

Vậy $\bar{f}' = \bar{f}$.

Hai nhóm X và Y được gọi là *đẳng cấu với nhau*, kí hiệu $X \cong Y$, nếu tồn tại một đẳng cấu $f : X \to Y$. Theo định lí 13 dễ dàng thấy rằng quan hệ đẳng cấu giữa các nhóm có các tính chất phản xạ, đối xứng và bắc cầu.

Nếu $f : X \to Y$ là một đơn cấu thì $f : X \to f(X)$ là một đẳng cấu. Do đó ta có $X \cong f(X)$.

Từ định lí đồng cấu nhóm suy ra : Nếu $f : X \to Y$ là một toàn cấu thì ta có $X/_{\text{Ker } f} \cong Y$.

§5. NHÓM SẮP THỨ TỰ

Cho (X, .) là một nhóm Abel và $\leq$ là một quan hệ thứ tự toàn phần trên X. Nếu (X,., $\leq$) là một nửa nhóm sắp thứ tự thì (X,., $\leq$) gọi là *một nhóm sắp thứ tự*, tức là mọi x, y, z $\in$ X, $x \leq y$ đều có $xz \leq yz$. Trong nhóm sắp thứ tự dễ thấy $x < y$ kéo theo $xz < yz$. Do đó mọi nhóm sắp thứ tự đều là sắp thứ tự nghiêm ngặt.

Trong nhóm sắp thứ tự $x < ax \Leftrightarrow 1_X < a$, do đó phần tử a của nhóm sắp thứ tự X gọi là *dương* nếu $1_X < a$.

Nhận xét 5. 1) Nếu (X,., $\leq$) là nhóm sắp thứ tự thì mọi nhóm con của X cũng là nhóm sắp thứ tự.

2) Trong nhóm sắp thứ tự ta có

$$a \leq b,\ c \leq d \Rightarrow ac \leq bd$$

$$a < b,\ c < d \Rightarrow ac < bd$$

Định lí 15. *Cho (X,., $\leq$) là một nhóm sắp thứ tự, P là tập các phần tử dương của nó. Khi đó*

1) $a, b \in P \Rightarrow ab \in P$;

2) Mọi $a \in X$ thì hoặc $a \in P$, hoặc $a^{-1} \in P$ hoặc $a = 1_X$;

3) $a, b \in X$, $a < b \Leftrightarrow ba^{-1} \in P$;

4) $1_X < a \Leftrightarrow a^{-1} < 1_X$.

CHỨNG MINH. 1) Mọi $a, b \in P$, $1_X < a$, $1_X < b \Rightarrow b < ab$, $1_X < b \Rightarrow 1_X < ab$. Vậy $ab \in P$.

2) Hiển nhiên $1_X \notin P$. Nếu a và a^{-1} đồng thời thuộc P thì theo 1) $1_X = aa^{-1} \in P$, ta gặp mâu thuẫn. Nếu cả a và a^{-1} đều

không thuộc P và $a \neq 1_X$ thì $a < 1_X$, $a^{-1} < 1_X \Rightarrow a < 1_X$, $1_X < a$
$\Rightarrow a = 1_X$, ta cũng gặp mâu thuẫn.

3) $a, b \in X$, $a < b \Leftrightarrow aa^{-1} < ba^{-1} \Leftrightarrow 1_X < ba^{-1} \Leftrightarrow ba^{-1} \in P$.

4) $1_X < a \Leftrightarrow 1_X a^{-1} < aa^{-1} \Leftrightarrow a^{-1} < 1_X$.

Định lí 16. *Cho (X,.) là một nhóm Abel, P là một tập con của X thỏa mãn các điều kiện*

1) $a, b \in P \Rightarrow ab \in P$;

2) Mỗi $a \in X$ thì hoặc $a \in P$, hoặc $a^{-1} \in P$ hoặc $a = 1_X$. Khi đó đặt $a \leq b$ nếu $a = b$ hoặc $ba^{-1} \in P$ thì $\leq$ là một quan hệ thứ tự trên X và (X,., $\leq$) là một nhóm sắp thứ tự.

CHỨNG MINH. Với mọi $a \in X$, $a \leq a$ nên $\leq$ có tính chất phản xạ. Nếu $a \leq b$, $b \leq a$ và $a \neq b$ thì $ba^{-1} \in P$, $ab^{-1} \in P \Rightarrow 1_X = (ba^{-1})(ab^{-1}) \in P$ ta gặp mâu thuẫn, do đó $a \leq b$, $b \leq a$ thì $a = b$, tức $\leq$ có tính phản xứng. Nếu $a \leq b$, $b \leq c$ và $a = b$ hoặc $b = c$ thì hiển nhiên $a \leq c$; nếu $a \neq b$ và $b \neq c$ thì $ba^{-1} \in P$ và $cb^{-1} \in P \Rightarrow ca^{-1} = (cb^{-1})(ba^{-1}) \in P \Rightarrow a \leq c$ vậy $\leq$ có tính chất bắc cầu.

Với mọi $a, b \in X$, nếu $ba^{-1} \in P$ thì $a < b$; nếu $(ba^{-1})^{-1} \in P$ thì $ab^{-1} \in P$ nên $b < a$; nếu $ba^{-1} = 1_X$ thì $a = b$. Do đó $\leq$ là quan hệ thứ tự toàn phần trên X.

Cuối cùng nếu $a, b, x \in X$, $a < b$ thì $ax < bx$ vì $(bx)(ax)^{-1} = ba^{-1} \in P$. Vậy (X,., $\leq$) là nhóm sắp thứ tự.

Nhận xét 6. Theo định lí 16, có thể định nghĩa : Nhóm Abel X gọi là sắp thứ tự nếu tồn tại một tập con $P \neq \emptyset$, gọi là tập dương, thỏa mãn hai tính chất 1) và 2) của định lí 16.

Ví dụ 10. Tập con $\mathbb{N}^*$ của nhóm $(\mathbb{Z},+)$ có các tính chất 1) và 2). Do đó với mọi $m, n \in \mathbb{Z}$ ta định nghĩa $m \le n$ nếu $m = n$ hoặc $n - m \in \mathbb{N}^*$ thì $\mathbb{Z}$ trở thành một nhóm sắp thứ tự. Thứ tự đó chính là thứ tự thông thường trên $\mathbb{Z}$.

BÀI TẬP CHƯƠNG II

2.1. Chứng minh rằng $\mathbb{Z}$ với phép toán $m \oplus n = m + n - 1$ là một nhóm Abel.

2.2. Chứng minh rằng $\mathbb{R} \setminus \left\{\frac{1}{2}\right\}$ với phép toán $x*y = x + y - 2xy$ là một nhóm Abel.

2.3. Chứng minh $X = \mathbb{R}^* \times \mathbb{R}$ với phép toán $(a, b)*(c, d) = (ac, bc + d)$ là một nhóm không giao hoán.

2.4. Chứng minh rằng G là một nhóm khi và chỉ khi

a) G là một nửa nhóm;

b) Với mọi $a, b \in G$ các phương trình

$$ax = b, \ xa = b$$

có nghiệm trong G.

2.5. Cho G là một nhóm Abel. Với mọi $n \ge 2$ kí hiệu

$$G_n = \left\{x \in G \mid x^n = 1_G\right\}.$$

Chứng minh rằng

a) G_n là nhóm con của G.

b) Nếu $(m, n) = 1$ thì $G_m \cap G_n = \left\{1_G\right\}$.

2.6. a) Chứng minh rằng một nửa nhóm G khác rỗng, hữu hạn là nhóm khi và chỉ khi mọi phần tử của nó đều thỏa mãn luật giản ước.

b) Chứng minh rằng mọi tập khác rỗng, hữu hạn, ổn định của nhóm G là một nhóm con của nhóm G.

2.7. Cho G là một nhóm có tính chất : $x^2 = 1_G$ với mọi $x \in G$. Chứng minh G là nhóm Abel.

2.8. Cho X là một nhóm. Tập con

$C(X) = \{z \in X \mid zx = xz$ với mọi $x \in X\}$ gọi là *tâm* của nhóm X. Chứng minh rằng C(X) là nhóm con của X.

2.9. Cho X là một nhóm và $a, b \in X$. Chứng minh rằng ab và ba có cùng một cấp.

2.10. Cho G là một nhóm hữu hạn cấp n. Chứng minh rằng

a) Mọi $x \in G$ đều có cấp là một ước số của n.

b) Mọi $x \in G$ đều có $x^n = 1_G$.

2.11. Chứng minh rằng mọi nhóm hữu hạn cấp nguyên tố đều là nhóm Cyclic, mọi phần tử khác phần tử trung hòa đều là phần tử sinh của nó.

2.12. Chứng minh rằng

a) Mọi nhóm cyclic cấp vô hạn đều có đúng 2 phần tử sinh.

b) Nếu một nhóm cyclic chỉ có một phần tử sinh thì nhóm đó có cấp ≤ 2.

2.13. Chứng minh rằng một nhóm không có nhóm con không tầm thường là nhóm cyclic.

2.14. Chứng minh rằng mọi nhóm cấp ≤ 5 đều là nhóm Abel.

2.15. Kí hiệu S_3 là nhóm các phép thế bậc 3 (Xem ví dụ 1c)).

Chứng minh rằng mọi nhóm con thực sự của nhóm S_3 đều là nhóm cyclic nhưng S_3 không là nhóm cyclic.

2.16. Cho X là một nhóm và $A \lhd X$, $B \lhd X$, $A \cap B = \{1_X\}$. Chứng minh rằng mọi $a \in A$, $b \in B$ đều có $ab = ba$.

2.17. Trong một nhóm X, ta gọi một phần tử có dạng $xyx^{-1}y^{-1}$ với $x, y \in X$ là một hoán tử của X. Nhóm con sinh bởi các hoán tử của X kí hiệu là $[X, X]$. Chứng minh rằng

a) $[X, X] \lhd X$ và $X/[X,X]$ là nhóm Abel.

b) Giả sử $A \lhd X$. Khi đó X/A là nhóm Abel $\Leftrightarrow [X, X] \subset A$.

2.18. Cho $A \lhd X$, $A \subset C(X)$. Chứng minh rằng nếu X/A là nhóm cyclic thì X là nhóm Abel.

2.19. Cho X là một nhóm và tập con $S \subset X$, $S \neq \emptyset$. Kí hiệu $xSx^{-1} = \{xsx^{-1} \mid s \in S\}$.

Ta gọi *chuẩn hóa* của S là tập

$N(S) = \{x \in X \mid xSx^{-1} = S\}$

và *tâm hoá* của S là tập

$C(S) = \{x \in X \mid xsx^{-1} = s \text{ với mọi } s \in S\}$.

Chứng minh rằng $C(S) \lhd N(S)$.

2.20. Trên tập $X = \mathbb{Z}^3$ xác định phép toán hai ngôi như sau

$$(k_1, k_2, k_3)(l_1, l_2, l_3) = (k_1 + (-1)^{k_3} l_1, k_2 + l_2, k_3 + l_3).$$

Chứng minh rằng

a) X cùng phép toán đó là một nhóm.

b) Nhóm con A sinh bởi phần tử (1,0,0) là chuẩn tắc.

2.21. Với mọi $n \in \mathbb{N}^*$, chứng minh $(\mathbb{Z},+) \cong (n\mathbb{Z},+)$.

2.22. Chứng minh rằng chỉ có một đồng cấu từ nhóm $(\mathbb{Q}, +)$ vào nhóm $(\mathbb{Z}, +)$ đó là đồng cấu tầm thường.

2.23. Chứng minh rằng không tồn tại một đẳng cấu từ $(\mathbb{R}, +)$ lên $(\mathbb{R}^*, .)$.

2.24. Chứng minh rằng ánh xạ $x \mapsto x^{-1}$ từ nhóm X vào chính nó là đẳng cấu nhóm khi và chỉ khi X là nhóm Abel.

2.25. Cho G_1 và G_2 là hai nhóm. Trên tích Descartes $G_1 \times G_2$ xác định phép toán

$$(x_1, y_1).(x_2, y_2) = (x_1x_2, y_1y_2).$$

a) Chứng minh $G_1 \times G_2$ cùng phép toán trên là một nhóm, gọi là nhóm tích của hai nhóm G_1 và G_2.

b) Cho G_1 và G_2 là nhóm cyclic hữu hạn cấp tương ứng là m và n. Chứng minh $G_1 \times G_2$ là nhóm cyclic $\Leftrightarrow (m, n) = 1$.

2.26. Chứng minh rằng với phép toán $m * n = m + n - 2$ và thứ tự $\leq$ thông thường, $(\mathbb{Z}, *, \leq)$ là một nhóm sắp thứ tự.

2.27. Chứng minh rằng nếu G là một nhóm sắp thứ tự thì G có vô hạn phần tử.

2.28. (Nhóm đối xứng hóa của một nửa nhóm). Cho X là một nửa nhóm cộng giao hoán, mọi phần tử đều thỏa mãn luật giản ước.

a) Chứng minh rằng quan hệ ~ trên X^2 xác định bởi

$$(a, b) \sim (c, d) \text{ nếu } a + d = b + c$$

là một quan hệ tương đương.

b) Kí hiệu $\overline{X} = X^2/_\sim$ là tập thương của X^2 theo quan hệ ~, phần tử của $\overline{X}$ chứa (a,b) là $\overline{(a,b)}$. Với mọi $\overline{(a,b)}$ và $\overline{(c,d)} \in \overline{X}$ đặt

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$

Chứng minh rằng quy tắc trên xác định một phép toán trên $\overline{X}$ và $(\overline{X},+)$ là một nhóm Abel.

c) Với mọi $a \in X$ chứng tỏ $\overline{(a+b,b)} \in \overline{X}$ không phụ thuộc vào $b \in X$. Chứng minh rằng $j : X \to \overline{X}$, $j(a) = \overline{(a+b, b)}$ là một đơn cấu nửa nhóm.

d) Đồng nhất $a \in X$ với $j(a) \in \overline{X}$. Chứng tỏ rằng mọi phần tử của $\overline{X}$ đều có dạng $a - b$ với $a, b \in X$.

Nhóm $\overline{X}$ gọi là *nhóm đối xứng hoá* của nửa nhóm X.

e) Chứng tỏ nhóm $(\mathbb{Z}, +)$ là đối xứng hoá của nửa nhóm $(\mathbb{N}, +)$; nhóm $(\mathbb{Q}^*_+, .)$ là đối xứng hoá của nửa nhóm $(\mathbb{N}^*, .)$.

CHƯƠNG III

VÀNH VÀ TRƯỜNG

§1. VÀNH

1. Định nghĩa và tính chất

Vành là một tập X cùng hai phép toán trên X, thường kí hiệu cộng và nhân thỏa mãn các tính chất

1) (X,+) là một nhóm Abel;

2) (X,.) là một nửa nhóm;

3) Phép nhân phân phối đối với phép cộng, tức là mọi $x, y, z \in X$ ta có

$$x(y + z) = xy + xz; \quad (y + z)x = yx + zx.$$

Một cách tương đương, ta có thể định nghĩa (X, +, .) là một vành nếu nó thỏa mãn các điều kiện sau

(R_1) Mọi $x, y, z \in X$, $(x + y) + z = x + (y + z)$.

(R_2) Mọi $x, y \in X$, $x + y = y + x$.

(R_3) Tồn tại $0_X \in X$, mọi $x \in X$, $x + 0_X = x$.

(R_4) Mọi $x \in X$, tồn tại $-x \in X$, $x + (-x) = 0_X$.

(R_5) Mọi $x, y, z \in X$, $(xy)z = x(yz)$.

(R_6) Mọi $x, y, z \in X$, $x(y + z) = xy + xz$, $(y + z)x = yx + zx$.

Nếu phép toán nhân của vành là giao hoán thì vành gọi là *vành giao hoán*. Nếp phép toán nhân có đơn vị thì vành gọi là *vành có đơn vị*.

Ví dụ 1. a) $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ là các vành giao hoán, có đơn vị.

b) $(\mathbb{Z}_k, +, .)$ là một vành giao hoán có đơn vị (Xem ví dụ 2, Chương II).

c) Cho (X, +) là một nhóm Abel. Kí hiệu End(X) là tập các đồng cấu nhóm từ X vào X (gọi là các *tự đồng cấu*). Trên End(X) xác định phép + và . như sau

f + g được xác định bởi

$$(f + g)(x) = f(x) + g(x) \text{ với mọi } x \in X.$$

f.g được xác định bởi

$$f.g(x) = f(g(x)) \text{ với mọi } x \in X.$$

Dễ dàng kiểm tra (End(X), +,.) là một vành có đơn vị nhưng nói chung là không giao hoán. Ta gọi vành này là *vành các tự đồng cấu* của nhóm Abel X.

d) Cho (X, +) là một nhóm Abel. Trên X xác định phép toán nhân

$$x.y = 0_X \text{ với mọi } x, y \in X.$$

Dễ dàng kiểm tra (X, +, .) là một vành giao hoán, nói chung không có đơn vị. Ta gọi vành này là *vành không* của nhóm Abel X.

Định lí 1. *Với mọi x, y, z của vành X ta có*

1) $x.0_X = 0_X.x = 0_X$

2) $(-x)y = x(-y) = -xy$

3) $(-x)(-y) = xy$

4) $x(y - z) = xy - xz$; $(y - z)x = yx - zx$.

CHỨNG MINH. 1) Ta có $x.0_X = x(0_X + 0_X) = x0_X + x0_X$. Do đó $x.0_X = 0_X$. Tương tự cũng có $0_X.x = 0_X$.

2) Vì $xy + (-x)y = (x + (-x))y = 0_X y = 0_X$ nên $(-x)y = -xy$

Tương tự ta cũng có $x(-y) = -xy$.

3) Theo 2) ta có $(-x)(-y) = -x(-y) = -(-xy) = xy$.

4) Theo 2) ta có $x(y - z) = x(y + (-z)) = xy + x(-z) = xy - xz$. Đẳng thức còn lại chứng minh tương tự.

Hệ quả. *Với mọi $m \in \mathbb{Z}$ và mọi phần tử x, y của vành X ta có $m(xy) = (mx)y = x(my)$.*

2. Vành con

Cho X là một vành và tập con A của X ổn định đối với hai phép toán của vành X. Nếu với phép toán cảm sinh, (A, +, .) là một vành thì vành A gọi là *vành con* của X.

Ví dụ 2. a) Cho X là một vành. Khi đó $\{0_X\}$ và X là vành con của X. Các vành con này gọi là các *vành con tầm thường* của X.

b) Vành $\mathbb{Z}$ các số nguyên là vành con của vành $\mathbb{Q}$ các số hữu tỉ.

c) Tập $2\mathbb{Z}$ là vành con của vành $\mathbb{Z}$ các số nguyên.

Định lí 2. *Tập con A của một vành X là vành con của vành X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow x + y \in A$ và $xy \in A$.

3) $x \in A \Rightarrow -x \in A$.

CHỨNG MINH. Theo định lí 1 Chương II, (A, +) là nhóm Abel $\Leftrightarrow$ $A \neq \emptyset$; $x, y \in A$ thì $x + y \in A$, $-x \in A$; (A,.) là nửa nhóm $\Leftrightarrow$ $x, y \in A$ thì $xy \in A$. Nếu A ổn định với các phép toán thì trong A phép nhân phân phối với phép cộng. Như vậy A là vành con $\Leftrightarrow$ A có các tính chất 1), 2), 3).

Định lí 3. *Tập con A của một vành X là vành con của vành X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \emptyset$

2) $x, y \in A \Rightarrow x - y \in A, xy \in A$.

Định lí 3 được chứng minh tương tự định lí 2 bằng cách áp dụng định lí 2, Chương II.

Cho S là một tập con của vành X. Ta gọi vành con của X sinh bởi tập S là *vành con nhỏ nhất chứa S*, kí hiệu là [S]. Như vậy vành con [S] sinh bởi tập S có hai tính chất đặc trưng

1) [S] là vành con;

2) Nếu A là vành con và $A \supset S$ thì $A \supset [S]$.

Định lí 4. *Với mọi tập con S của vành X đều tồn tại và duy nhất vành con [S] sinh bởi tập S.*

CHỨNG MINH. Gọi $\mathscr{B}$ là họ tất cả các vành con của vành X chứa S. Vì $x \in \mathscr{B}$ nên $\mathscr{B} \neq \emptyset$. Ta sẽ chứng minh

$$[S] = \bigcap_{B \in \mathscr{B}} B,$$

tức là cần chứng minh $A = \bigcap_{B \in \mathscr{B}} B$ là vành con của X. Thật vậy, $0_X \in B$ với mọi B nên $0_X \in A$. Nếu $x, y \in A$ thì $x, y \in B$ với mọi B. Vì B là vành con nên $x - y \in B$ và $xy \in B$ với mọi B. Điều đó có nghĩa là $x - y \in A$ và $xy \in A$. Theo định lí 3, A là vành con.

Ví dụ 3. Với mọi $k \in \mathbb{N}$, $k\mathbb{Z}$ là vành con của $\mathbb{Z}$ sinh bởi tập một phần tử {k}.

§2. IDEAL. VÀNH THƯƠNG

1. Định nghĩa và tính chất của ideal

Cho X là một vành. Vành con A của X gọi là *ideal trái (phải)* nếu mọi $x \in X$, $a \in A$ đều có $xa \in A$ ($ax \in A$). Vành con A gọi là *ideal* nếu nó vừa là ideal phải, vừa là ideal trái.

Nếu vành giao hoán thì mọi ideal trái hay phải của X đều là ideal.

Ví dụ 4. a) Với mọi vành X thì $\{0_X\}$ và X là hai ideal của X, gọi là các *ideal tầm thường*.

b) Với mọi $k \in \mathbb{N}$, $k\mathbb{Z}$ là ideal của $\mathbb{Z}$.

c) $\mathbb{Z}$ là vành con của $\mathbb{Q}$ nhưng $\mathbb{Z}$ không là ideal của $\mathbb{Q}$. Từ định lí 2 và 3 ta có hai định lí sau

Định lí 5. *Tập con A của vành X là ideal trái (phải) của X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \varnothing$

2) $a, b \in A \Rightarrow a + b \in A$

3) $a \in A \Rightarrow -a \in A$

4) $x \in X, a \in A \Rightarrow xa \in A$ ($ax \in A$)

Định lí 6. *Tập con A của vành X là ideal trái (phải) của X khi và chỉ khi thỏa mãn các điều kiện sau*

1) $A \neq \varnothing$.

2) $a, b \in A \Rightarrow a - b \in A$.

3) $x \in A, a \in A \Rightarrow xa \in A$ ($ax \in A$).

2. Ideal sinh bởi một tập

Cho S là một tập con của vành X. Tương tự như chứng minh định lí 4 dễ dàng thấy rằng giao của tất cả các ideal trái (phải, hai phía) của X chứa S cũng là một ideal trái (phải, hai phía). Ideal này là ideal trái (phải, hai phía) nhỏ nhất chứa tập S, nên gọi là *ideal trái (phải, hai phía) sinh bởi tập S.*

Ideal (hai phía) sinh bởi tập S kí hiệu là <S>.

Chú ý rằng nói chung $<S> \neq [S]$.

Ideal sinh bởi tập một phần tử {a} gọi là *ideal sinh bởi phần tử a*, kí hiệu là <a>. Nếu tồn tại phần tử a sao cho ideal A = <a> thì ideal A gọi là *ideal chính.*

Dễ dàng thấy rằng nếu vành X có đơn vị và a là phần tử khả nghịch của X thì <a> = X.

Định lí 7. *Nếu X là một vành có đơn vị thì ideal trái sinh bởi phần tử $a \in X$ là*

$$Xa = \{xa \mid x \in X\}$$

và ideal phải sinh bởi a là

$$aX = \{ax \mid x \in X\}.$$

CHỨNG MINH. Ta chỉ chứng minh Xa là ideal trái sinh bởi a. Trước hết ta chứng tỏ Xa là ideal trái chứa a. Thật vậy $a = 1_X a \in Xa$. Với mọi b, c ∈ Xa, tồn tại $b', c' \in X$ sao cho b = b'a, c = c'a, từ đó

$$b - c = (b' - c')a \in Xa.$$

Với mọi $x \in X$ và $b = b'a \in Xa$ ta có

$$xb = x(b'.a) = (xb')a \in Xa.$$

Vậy Xa là ideal trái của X, chứa a.

Bây giờ ta sẽ chỉ ra mọi ideal trái A_t chứa a đều chứa Xa. Thật vậy, vì $a \in A_t$ và A_t là ideal trái nên mọi $x \in X$ ta có $xa \in A_t$. Vậy $Xa \subset A_t$.

3. Vành thương

Cho X là một vành và A là một ideal của nó. Vì phép cộng giao hoán nên A là một nhóm con chuẩn tắc của nhóm (X, +). Từ đó ta có nhóm thương X/A với phép toán cộng.

$$(x + A) + (y + A) = (x + y) + A.$$

Rõ ràng $(X/A, +)$ là một nhóm Abel. Trên X/A ta đặt

$$(x + A).(y + A) = xy + A$$

Nếu $x + A = x' + A$, $y + A = y' + A$ thì $x' - x = a \in A$

$y' - y = b \in A$. Vì A là ideal nên

$$x'y' - xy = (a + x)(b + y) - xy = xb + ay + ab \in A.$$

Từ đó $$x'y' + A = xy + A$$

Vậy cách đặt trên cho ta một phép toán nhân trên X/A.

Dễ dàng kiểm tra $(X/A, +, .)$ là một vành.

Vành này được gọi là *vành thương của X theo ideal A*.

Nếu vành X có đơn vị thì vành X/A có đơn vị là $1_X + A$. Nếu vành X giao hoán thì vành X/A cũng giao hoán.

Ví dụ 5. Với mọi $k \in \mathbb{N}$, $k\mathbb{Z}$ là ideal của $\mathbb{Z}$. Vành thương $\mathbb{Z}/k\mathbb{Z}$ chính là vành $\mathbb{Z}_k$ (Ví dụ 1, b)).

§3. ĐỒNG CẤU VÀNH

1. Định nghĩa và tính chất

Cho X và Y là hai vành. Một ánh xạ $f : X \to Y$ gọi là một *đồng cấu vành* nếu với mọi $x, y \in X$ ta có

$$f(x + y) = f(x) + f(y).$$
$$f(xy) = f(x)\, f(y).$$

Như vậy một đồng cấu vành $f : X \to Y$ là một đồng cấu từ nhóm cộng X vào nhóm cộng Y và là một đồng cấu từ nửa nhóm nhân X vào nửa nhóm nhân Y. Vì f là đồng cấu nhóm cộng nên

$$f(0_X) = 0_Y, \quad f(-x) = -f(x).$$

Đồng cấu vành f được gọi tương ứng là *đơn cấu, toàn cấu, đẳng cấu* nếu ánh xạ f là đơn ánh, toàn ánh, song ánh.

Một đồng cấu từ vành X vào chính nó được gọi là một *tự đồng cấu*.

Ví dụ 6. a) Cho X là một vành có đơn vị 1_X. Ánh xạ $f : \mathbb{Z} \to X$ xác định bởi $f(m) = m.1_X$ là một đồng cấu từ vành $\mathbb{Z}$ các số nguyên vào vành X. Thật vậy với mọi $m, n \in \mathbb{Z}$ ta có

$$f(m + n) = (m + n)1_X = m1_X + n1_X = f(m) + f(n)$$

$$f(m.n) = (m.n)1_X = (m.1_X)(n.1_X) = f(m)f(n).$$

b) Cho X là một vành. Ánh xạ đồng nhất $I_X : X \to X$ là đẳng cấu vành.

c) Cho A là một vành con của vành X. Ánh xạ $j_A : A \to X$, $j_A(x) = x$ là đơn cấu vành, gọi là *phép nhúng chính tắc* A vào X.

d) Cho X là một vành và A là một ideal của X. Ánh xạ $p : X \to X/A$, $p(x) = x + A$ là một toàn cấu vành, gọi là *toàn cấu chính tắc* X lên X/A.

e) Cho X và Y là hai vành. Ánh xạ $f : X \to Y$, $f(x) = 0_Y$ với mọi $x \in X$ là đồng cấu vành, gọi là *đồng cấu không*.

Tương tự như đồng cấu nhóm, ta có

Định lí 8. *1) Cho $f : X \to Y$, $g : Y \to Z$ là các đồng cấu vành. Khi đó $gof : X \to Z$ là đồng cấu vành.*

2) Cho $f : X \to Y$ là đẳng cấu vành. Khi đó ánh xạ ngược $f^{-1} : Y \to X$ cũng là đẳng cấu vành.

2. Ảnh và hạt nhân của đồng cấu vành

Vì đồng cấu vành là một đồng cấu của nhóm cộng và là một đồng cấu của nửa nhóm nhân nên theo kết quả tương ứng của đồng cấu nhóm và đồng cấu nửa nhóm ta có

Định lí 9. *Cho $f : X \to Y$ là một đồng cấu vành. Khi đó*

1) A là vành con của vành X thì f(A) là vành con của vành Y.

2) B là vành con của vành Y thì $f^{-1}(B)$ là vành con của vành X.

Cho $f : X \to Y$ là một đồng cấu vành. Theo định lí 9, f(X) là một vành con của Y, ta gọi vành con này là *ảnh* của f, kí hiệu là Imf; $f^{-1}\left(\left\{0_Y\right\}\right) = f^{-1}\left(0_Y\right)$ là một vành con của X, ta gọi vành con này là *hạt nhân* của f, kí hiệu là Ker f.

Định lí 10. *Với mọi đồng cấu vành $f : X \to Y$, Ker f là một ideal của vành X.*

CHỨNG MINH. Vì Ker f là một vành con nên ta chỉ còn phải chứng minh mọi $x \in X$ và $a \in$ Ker f đều có xa và ax $\in$ Ker f. Vì

$$f(xa) = f(x).f(a) = f(x)0_Y = 0_Y$$

$$f(ax) = f(a).f(x) = 0_Y f(x) = 0_Y$$

nên ta có điều cần chứng minh.

3. Định lí đồng cấu vành

Định lí 11. *Cho $f : X \to Y$ là một đồng cấu vành, $p : X \to X/_{Ker f}$ là toàn cấu chính tắc từ vành X lên vành thương $X/_{Ker f}$. Khi đó tồn tại duy nhất đơn cấu vành $\bar{f} : X/_{Ker f} \to Y$ sao cho $\bar{f} o p = f$.*

CHỨNG MINH. Sự tồn tại : Đặt A = Ker f. Ta sẽ chỉ ra $\bar{f} : X/_A \to Y$, $\bar{f}(x + A) = f(x)$ có các tính chất đòi hỏi. Thật vậy, hiển nhiên $\bar{f}$ là ánh xạ. Với mọi $x + A, y + A \in X/_A$ ta có

$$\bar{f}((x + A) + (y + A)) = \bar{f}(x + y + A) = f(x + y)$$
$$= f(x) + f(y) = \bar{f}(x + A) + \bar{f}(y + A);$$

$$\bar{f}((x + A) . (y + A)) = \bar{f}(xy + A) = f(xy)$$
$$= f(x) f(y) = \bar{f}(x + A) \bar{f}(y + A)$$

nên $\bar{f}$ là đồng cấu. Giả sử $x + A, y + A \in X/_A$, $x + A \neq y + A \Rightarrow y - x \notin A \Rightarrow f(y - x) \neq 0 \Rightarrow f(x) \neq f(y) \Rightarrow \bar{f}(x + A) \neq \bar{f}(y + A)$ nên $\bar{f}$ là đơn cấu. Cuối cùng với mọi $x \in X$ ta có $\bar{f} o p(x) = \bar{f}(x + A) = f(x)$ nên $\bar{f} o p = f$.

Tính duy nhất : Nếu $\bar{f}' : X/_A \to Y$ cũng có tính chất đòi hỏi thì $\bar{f}' o p = f$. Từ đó với mọi $x + A \in X/_A$ ta có

$$\bar{f}'(x + A) = \bar{f}'(p(x)) = f(x) = \bar{f}(x + A). \text{ Vậy } \bar{f}' = \bar{f}.$$

Hai vành X và Y được gọi là *đẳng cấu với nhau*, kí hiệu $X \cong Y$, nếu tồn tại một đẳng cấu $f : X \to Y$. Theo định lí 8 dễ thấy rằng quan hệ đẳng cấu giữa các vành có các tính chất phản xạ, đối xứng và bắc cầu.

Nếu $f : X \to Y$ là một đơn cấu vành thì $f : X \to f(X)$ là một đẳng cấu vành. Do đó ta có $X \cong f(X)$.

Từ định lí đồng cấu vành suy ra : Nếu $f : X \to Y$ là một toàn cấu vành thì ta có $X/_{Ker f} \cong Y$.

§4. VÀNH SẮP THỨ TỰ

1. Định nghĩa và tính chất

Cho (X, +, .) là một vành giao hoán và $\leq$ là một quan hệ thứ tự toàn phần trên X. Khi đó (X, +,., $\leq$) gọi là *một vành sắp thứ tự* nếu mọi x, y, z $\in$ X ta có

1) $x \leq y \Rightarrow x + z \leq y + z$

2) $0 \leq x, 0 \leq y \Rightarrow 0 \leq xy$.

Vành được gọi là *sắp thứ tự nghiêm ngặt* nếu 2) được thay bởi

2') $0 < x, 0 < y \Rightarrow 0 < xy$.

Ở đây như thông lệ $x < y$, nghĩa là $x \leq y$ và $x \neq y$.

Ví dụ 7. Vành $\mathbb{Z}$ các số nguyên với quan hệ thứ tự thông thường là vành sắp thứ tự nghiêm ngặt.

Trong một vành sắp thứ tự nghiêm ngặt X ta gọi phần tử $a \in X$ là *phần tử dương* nếu $0 < a$.

Kí hiệu P là tập các phần tử dương của vành sắp thứ tự X.

Định lí 12. *Trong một vành sắp thứ tự nghiêm ngặt X ta có*

1) $a, b \in P \Rightarrow a + b \in P$, $a.b \in P$;

2) Mọi $a \in X$ *thì hoặc* $a \in P$, *hoặc* $-a \in P$ *hoặc* $a = 0_X$;

3) $a, b \in X$, $a < b \Leftrightarrow b - a \in P$;

4) $0 < a \Leftrightarrow -a < 0$.

CHỨNG MINH. Nhận được từ định lí 15 Chương II.

Dễ dàng chứng minh định lí sau đây :

Định lí 13. *Một vành giao hoán X được sắp thứ tự nghiêm ngặt khi và chỉ khi trong X tồn tại một tập con P có các tính chất 1), 2) và 3) của định lí 12. Quan hệ thứ tự để biến X thành một vành sắp thứ tự là quan hệ*

$$a \leq b \text{ nếu } a = b \text{ hoặc } b - a \in P.$$

§5. TRƯỜNG

1. Định nghĩa và tính chất

Ta gọi *trường* là một vành giao hoán, có đơn vị, có nhiều hơn một phần tử và mọi phần tử khác không đều khả nghịch.

Cho X là một trường, kí hiệu 0 là *phần tử không*, 1 là *phần tử đơn vị*.

Trước hết ta nhận xét rằng $0 \neq 1$. Thật vậy, trong x tồn tại $x \neq 0$, do đó tồn tại x^{-1}. Từ đó $x.x^{-1} \neq 0.x^{-1} \Rightarrow 1 \neq 0$.

Phần tử $x \neq 0$ của một vành X gọi là *ước của không* nếu tồn tại $y \in X$, $y \neq 0$ sao cho $xy = 0$.

Ta nhận xét rằng : *Mọi trường X đều không có ước của không.* Thật vậy, mọi $x \in X$, $x \neq 0$, nếu có $y \in X$ sao cho $xy = 0$ thì $x^{-1}xy = x^{-1}0 \Rightarrow y = 0$. Do đó x không là ước của không.

Đặt $X^* = X \setminus \{0\}$. Theo các nhận xét trên X^* ổn định với phép toán nhân, $1 \in X^*$. Nếu $x \in X^*$ thì tồn tại $x^{-1} \in X^*$. Do đó $(X^*,.)$ là một nhóm Abel.

Như vậy, một cách tương đương, có thể định nghĩa : *(X,+,.) là một trường nếu*

1) *X cùng phép toán cộng là một nhóm Abel;*

2) *$X^* = X \setminus \{0\}$ cùng với phép nhân là một nhóm Abel;*

3) *Phép nhân phân phối đối với phép cộng.*

Ví dụ 8. a) Với phép cộng và nhân thông thường $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$ là các trường.

b) $(\mathbb{Z}_p,+,.)$ với p nguyên tố là trường.

Định lí 14. *Vành giao hoán, có đơn vị, có nhiều hơn một phần tử X là một trường khi và chỉ khi X có đúng hai ideal tầm thường là {0} và X.*

CHỨNG MINH. Giả sử X là một trường và A là một ideal bất kì của X, $A \neq \{0\}$. Khi đó tồn tại $a \in A$, $a \neq 0$. Suy ra $1 = a^{-1}a \in A$. Với mọi $x \in X$ ta có $x.1 \in A$ nên $A = X$. Vậy X chỉ có đúng hai ideal.

Ngược lại, giả sử X là vành giao hoán, có đơn vị, có nhiều hơn một phần tử và có đúng hai ideal. Với mọi $x \in X$, $x \neq 0$, theo định lí 7, xX là ideal của X sinh bởi x. Vì $xX \neq \{0\}$ nên $xX = X$. Từ đó tồn tại $y \in X$ để $xy = 1$. Vì vành X giao hoán nên x có phần tử nghịch đảo là y.

2. Trường con

Cho X là một trường. Tập con A của X gọi là một *trường con* của X nếu A ổn định đối với hai phép toán trong X và A cùng với hai phép toán cảm sinh tạo thành một trường.

Ví dụ 9. $\mathbb{Q}$ là trường con của trường con của trường số thực $\mathbb{R}$. Từ các định lí 1 và 2 Chương II ta có hai định lí sau

Định lí 15. *Tập con A của trường X có nhiều hơn một phần tử là trường con của trường X khi và chỉ khi thỏa mãn các điều kiện*

1) $x, y \in A \Rightarrow x + y \in A, xy \in A$.

2) $x \in A \Rightarrow -x \in A$.

3) $x \in A, x \neq 0 \Rightarrow x^{-1} \in A$.

Định lí 16. *Tập con A của trường X có nhiều hơn một phần tử là trường con của trường X khi và chỉ khi thỏa mãn các điều kiện*

1) $x, y \in A \Rightarrow x - y \in A$.

2) $x, y \in A, y \neq 0 \Rightarrow xy^{-1} \in A$.

Ví dụ 10. $\mathbf{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\right\}$ là trường con của trường số thực $\mathbb{R}$.

Thật vậy với mọi $x = a + b\sqrt{2}$ và $y = c + d\sqrt{2}$ thuộc $\mathbf{Q}\left(\sqrt{2}\right)$ ta có

$$x - y = (a - c) + (b - d)\sqrt{2} \in \mathbf{Q}\left(\sqrt{2}\right)$$

Nếu thêm $y \neq 0$ thì

$$xy^{-1} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2}$$

$$= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} \in \mathbf{Q}(\sqrt{2}).$$

Vậy theo định lí 16, $\mathbf{Q}\left(\sqrt{2}\right)$ là trường con của trường $\mathbb{R}$.

4. Miền nguyên

Ta gọi một vành giao hoán, có đơn vị, nhiều hơn một phần tử, không có ước của không là một *miền nguyên*.

Theo nhận xét trong 1. thì mọi trường đều là miền nguyên. Vành số nguyên $\mathbb{Z}$ là ví dụ về một miền nguyên nhưng không phải là trường.

Trong miền nguyên mọi phần tử khác không đều thỏa mãn luật giản ước đối với phép nhân. Thật vậy, với mọi $a \neq 0$:

$$ab = ac \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c.$$

5. Trường sắp thứ tự

Cho X là một trường và một quan hệ thứ tự toàn phần $\leq$ trên X. Khi đó X được gọi là một *trường sắp thứ tự* nếu nó là một vành sắp thứ tự. Dễ dàng thấy rằng *mọi miền nguyên sắp thứ tự đều là sắp thứ tự nghiêm ngặt.*

Cho X là một trường (hoặc vành) sắp thứ tự. Với mọi $x \in X$ ta gọi giá trị tuyệt đối của x là phần tử $|x| \in X$ được xác định bởi

$$|x| = \begin{cases} x \text{ nếu } 0 < x \\ 0 \text{ nếu } x = 0 \\ -x \text{ nếu } x < 0 \end{cases}$$

Với mọi $x, y \in X$ ta có các tính chất sau

1) $0 \le |x|, |x| = 0 \Leftrightarrow x = 0$

2) $|xy| = |x||y|$

3) $|x + y| \le |x| + |y|$

4) $||a| - |b|| \le |a - b|$.

BÀI TẬP CHƯƠNG III

3.1. Cho X là một vành và $x \in X$. Chứng minh rằng với mọi $n \in \mathbb{N}^*$

$$(-x)^n = \begin{cases} x^n \text{ nếu n chẵn} \\ -x^n \text{ nếu n lẻ.} \end{cases}$$

3.2. Trong một vành có đơn vị X chứng minh rằng nếu x khả nghịch thì $-x$ cũng khả nghịch và $(-x)^{-1} = -x^{-1}$.

3.3. Trên tập $\mathbb{Z} \times \mathbb{Z}$ định nghĩa các phép toán

$$(m, n) + (p, q) = (m + p, n + q)$$

$$(m, n).(p, q) = (mp, mq + np + nq).$$

Chứng minh rằng với các phép toán trên $\mathbb{Z} \times \mathbb{Z}$ là vành giao hoán, có đơn vị.

3.4. Cho X là một vành, S là một tập hợp. Kí hiệu X^S là tập các ánh xạ từ S đến X. Với mọi f, g $\in X^S$ ta định nghĩa f + g và f.g xác định bởi

$$(f + g)(s) = f(s) + g(s),\ (f.g)(s) = f(s).g(s)$$

với mọi $s \in S$. Chứng minh rằng với các phép toán trên X^S là một vành. Nếu vành X giao hoán hay có đơn vị thì vành X^S cũng có tính chất đó.

3.5. Các tập sau đây, tập nào là vành con của vành $\mathbb{R}$:

a) $\{m + n\sqrt{5} \mid m, n \in \mathbb{Z}\}$?

b) $\{m + n\sqrt[3]{5} \mid m, n \in \mathbb{Z}\}$?

c) $\{m + n\sqrt[3]{5} + p\sqrt[3]{25} \mid m, n, p \in \mathbb{Z}\}$?

3.6. Cho X là một vành. Ta gọi tâm của X là tập

$$C(X) = \{a \in X \mid ax = xa \text{ với mọi } x \in X\}.$$

Chứng minh rằng C(X) là vành con giao hoán của X.

3.7. Trong một vành X nếu có số nguyên m > 0 sao cho

$$mx = 0_X \text{ với mọi } x \in X \ (*)$$

thì số nguyên dương s nhỏ nhất thỏa mãn (*) gọi là đặc số của vành X.

Nếu không có m > 0 thỏa mãn (*) thì m = 0 là số duy nhất thỏa mãn (*), trường hợp này ta nói vành có đặc số 0.

Chứng minh rằng

a) Nếu vành X có đặc số $s \neq 0$ thì mọi phần tử không phải ước của không trong vành đều có cấp bằng s.

b) Nếu vành X có đặc số s = 0 thì mọi phần tử không phải ước của không trong vành đều có cấp vô hạn.

c) Nếu vành X có đơn vị $1_X \neq 0_X$ thì đặc số của vành X chính là cấp của phần tử 1_X trong nhóm (X, +), tức 0 là số dương nhỏ nhất để $s.1_X = 0_X$.

3.8. Một vành X gọi là *vành Bulle* nếu mọi phần tử của nó đều có tính chất lũy đẳng, tức là $x^2 = x$. Chứng minh rằng vành Bulle là vành giao hoán, có đặc số bằng 2.

3.9. Cho X là một vành. Với mọi $m \in \mathbb{Z}$ chứng minh các tập sau đây là ideal của X :

a) $mX = \{mx \mid x \in X\}$;

b) $A = \{x \in X \mid mx = 0\}$.

3.10. Cho A và B là hai ideal của vành X. Chứng minh rằng

$$A + B = \{a + b \mid a \in A, b \in B\}$$

cũng là một ideal của X.

3.11. Cho X là một vành, I_0 là ideal của X sinh bởi các phần tử dạng xy − yx, x, y ∈ X.

a) Chứng minh X/I_0 là vành giao hoán.

b) Với mọi ideal I của X, X/I là vành giao hoán $\Leftrightarrow I_0 \subset I$.

3.12. Tìm tất cả các tự đồng cấu của vành số nguyên $\mathbb{Z}$.

3.13. Kí hiệu $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$, n = 7; 11.

Chứng minh rằng

a) $\mathbb{Q}(\sqrt{7})$ và $\mathbb{Q}(\sqrt{11})$ là trường con của trường $\mathbb{R}$.

b) Ánh xạ f : $\mathbf{Q}(\sqrt{7}) \to \mathbf{Q}(\sqrt{11})$

$$a + b\sqrt{7} \mapsto a + b\sqrt{11}$$

không phải là đẳng cấu trường.

c) Không tồn tại một đẳng cấu nào giữa $\mathbf{Q}(\sqrt{7})$ và $\mathbf{Q}(\sqrt{11})$.

3.14. Cho A là một ideal của vành giao hoán, có đơn vị $1 \neq 0$ X. Ideal A gọi là *nguyên tố* nếu mọi x, y $\in$ X, xy $\in$ A thì x $\in$ A hoặc y $\in$ A. Ideal A gọi là *tối đại* nếu A $\neq$ X và nếu M là một ideal của X, $A \subset M \subset X$ thì M = A hoặc M = X.

Chứng minh rằng

a) Ideal $\{0\}$ là nguyên tố $\Leftrightarrow$ X là miền nguyên.

b) Ideal $\{0\}$ là tối đại $\Leftrightarrow$ X là một trường.

c) Ideal P là nguyên tố $\Leftrightarrow$ X/P là miền nguyên.

d) Ideal M là tối đại $\Leftrightarrow$ X/M là một trường.

e) M là ideal tối đại thì M là ideal nguyên tố.

3.15. Cho A là một vành con có nhiều hơn một phần tử của một trường F. Chứng minh rằng trường con của F sinh bởi A (tức là trường con nhỏ nhất của F chứa A) là tập

$$F(A) = \{xy^{-1} \mid x, y \in A, y \neq 0\}.$$

3.16. Cho X là một vành. Trên tập $\mathbb{Z} \times X$ xét các phép toán

$$(m, x) + (n, y) = (m + n, x + y)$$

$$(m, x) . (n, y) = (mn, nx + my + xy)$$

Chứng minh rằng

a) ($\mathbb{Z} \times X$, +,.) là một vành có đơn vị.

b) Ánh xạ $h : X \to \mathbb{Z} \times X$, $h(x) = (0,x)$ là đơn cấu vành. Do đó một vành bất kì đều có thể coi là vành con của một vành có đơn vị.

3.17. (Trường các thương của một miền nguyên). Cho A là một miền nguyên. Kí hiệu $A^* = A \setminus \{0_A\}$. Trên tích Descartes $A \times A^*$ xét quan hệ

$$(x, x') \sim (y, y') \text{ nếu } xy' = yx'.$$

a) Chứng tỏ $\sim$ là một quan hệ tương đương trên $A \times A^*$. Kí hiệu tập thương $A \times A^*/_\sim$ là F(A). Kí hiệu phần tử của F(A) chứa (x, x') là $\frac{x}{x'}$.

b) Trên tập F(A) đặt

$$\frac{x}{x'} + \frac{y}{y'} = \frac{xy' + yx'}{x'y'}$$

$$\frac{x}{x'} + \frac{y}{y'} = \frac{xy}{x'y'}$$

Chứng tỏ các quy tắc đó xác định các phép toán trên F(A) và (F(A), +,.) là một trường.

c) Chứng tỏ rằng với mọi $x \in A$, phần tử $\frac{xy'}{y'} \in F(A)$ không phụ thuộc vào $y' \in A^*$. Chứng minh ánh xạ $j : A \to F(A)$, $j(x) = \frac{xy'}{y'}$ là một đơn cấu vành.

d) Đồng nhất $x \in A$ với $\frac{xy'}{y'} \in F(A)$. Ta có A là một vành con của trường F(A). Chứng tỏ mọi $\frac{x}{x'} \in F(A)$ đều có dạng $x.x'^{-1}$, $x, x' \in A$. (Hãy liên hệ với bài tập 3.15).

e) Hãy chứng tỏ $\mathbb{Q}$ là trường các thương của $\mathbb{Z}$.

3.18. Kí hiệu $\mathcal{M}_2(F)$ là tập các ma trận vuông cấp hai trên một trường F. Tức là tập các phần tử A có dạng

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ a, b, c, d \in F.$$

Hai ma trận gọi là *bằng nhau* nếu có tất cả các phần tử tương ứng của chúng bằng nhau.

Với mọi $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ và $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathcal{M}_2(F)$ ta định nghĩa

$$A_1 + A_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

$$A_1 . A_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

a) Chứng minh rằng $\mathcal{M}_2(F)$ với phép cộng và phép nhân như trên là một vành có đơn vị.

b) Với mọi $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(F)$ ta định nghĩa định thức của A là phần tử

$$|A| = ad - bc.$$

Chứng minh rằng với mọi $A_1, A_2 \in \mathcal{M}_2(F)$ ta có

$$|A_1 . A_2| = |A_1| . A_2 .$$

c) Ma trận $A \in \mathcal{M}_2(F)$ gọi là *không suy biến* nếu $|A| \neq 0$.

Chứng minh rằng A khả nghịch $\Leftrightarrow$ A không suy biến.

3.19. (Trường số phức) Trên vành $\mathcal{M}_2(\mathbb{R})$ các ma trận vuông cấp hai trên trường $\mathbb{R}$ xét tập con

$$\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}.$$

a) Chứng minh rằng $\mathbb{C}$ là một trường con của vành $\mathcal{M}_2(\mathbb{R})$.

b) Chứng minh rằng ánh xạ $j : \mathbb{R} \to \mathbb{C}$, $j(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ là một đơn cấu

c) Đặt $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, đồng nhất $j(a)$ với a, chứng minh

$$i^2 = -1 \text{ và } \mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}.$$

Mỗi phần tử của $\mathbb{C}$ gọi là một *số phức*.

d) Với mọi $a_1 + ib_1, a_2 + ib_2 \in \mathbb{C}$ chứng minh :

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$$

$$(a_1 + ib_1)(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$$

e) Kí hiệu $z = a + ib$ và gọi $\bar{z} = a - ib$ là *số phức liên hiệp* của z. Với mọi $z_1, z_2 \in \mathbb{C}$ chứng minh

$$\overline{\overline{z_1}} = z_1,\ \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1z_2} = \overline{z_1}\ \overline{z_2}.$$

f) Đặt $|z| = (z.\bar{z})^{1/2}$ và gọi là *môđun của số phức z*. Với mọi $z, z_1, z_2 \in \mathbb{C}$ ta có

$$|z| \geq 0, z = 0 \Leftrightarrow z = 0$$

$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

$$|z_1z_2| = |z_1||z_2|.$$

$$\big||z_1| - |z_2|\big| \leq |z_1 - z_2|.$$

3.20. (Thể quaternion) Trên vành $\mathcal{M}_2(\mathbb{C})$ các ma trận vuông cấp hai trên trường $\mathbb{C}$ xét tập con

$$2 = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}.$$

a) Chứng minh rằng 2 là một thể con của vành $\mathcal{M}_2(\mathbb{C})$. (*Thể* là một vành có đơn vị, có nhiều hơn một phần tử, mọi phần tử khác không đều khả đảo).

b) Đặt $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Chứng minh rằng

$I^2 = J^2 = K^2 = -1$; $IJ = -JI = K$, $JK = -KJ = I$, $IK = -KI = J$.

c) Đồng nhất số thực a với $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in 2$. Chứng tỏ mọi phần tử của 2 đều có dạng

$$a_1 + a_2 I + b_1 J + b_2 K,\ a_1, a_2, b_1, b_2 \in \mathbb{R}.$$

Thể 2 được gọi là *thể quaternion*. Theo b) 2 không giao hoán, do đó 2 không phải là trường.

3.21. Trong một trường sắp thứ tự, chứng minh rằng

a) $0 < 1$;

b) $0 < a \Leftrightarrow 0 < a^{-1}$.

c) $a < b < 0 \Leftrightarrow 0 > a^{-1} > b^{-1}$.

d) $a < b$ thì tồn tại vô số x để $a < x < b$.

3.22. Chứng minh rằng không có một quan hệ $\leq$ để biến trường số phức $\mathbb{C}$ thành một trường sắp thứ tự.

CHƯƠNG IV

MỘT VÀI LỚP VÀNH ĐẶC BIỆT

§1. SỐ HỌC TRONG MIỀN NGUYÊN

1. Khái niệm chia hết

Cho X là một miền nguyên, a, b $\in$ X và b $\neq$ 0. Nếu tồn tại c $\in$ X sao cho a = bc thì ta viết

$$b \mid a \text{ hoặc } a \,\vdots\, b$$

và gọi là *a chia hết cho b*. Thay cho cách gọi "a chia hết cho b" ta còn gọi một trong các cách sau đây : *"a là bội của b"*, *"b chia hết a"* hoặc *"b là ước của a"*.

Hai phần tử a và b của một miền nguyên gọi là *liên kết* nếu đồng thời có a | b và b | a.

Định lí 1. *Hai phần tử a, b của một miền nguyên X liên kết khi và chỉ khi a $\neq$ 0, b $\neq$ 0 và tồn tại u$\in$X, u khả nghịch sao cho a = bu.*

CHỨNG MINH. Nếu a | b và b | a thì a $\neq$ 0 và b $\neq$ 0 và tồn tại u, v $\in$ X sao cho a = bu và b = av. Từ đó

$$a = auv \Rightarrow uv = 1 \Rightarrow u, v \text{ khả nghịch}$$

Ngược lại, nếu a = bu thì b | a. Mặt khác do u khả nghịch nên $b = a.u^{-1}$, tức là cũng có a | b. Vậy a và b liên kết.

Từ định lí 1 suy ra quan hệ liên kết là một quan hệ tương đương trên tập $X^* = X\setminus\{0\}$. Cũng do định lí 1 ta còn gọi hai phần tử liên kết là *hai phần tử khác nhau một phần tử khả nghịch*.

Nếu $b \mid a$, b không khả nghịch, b không liên kết với a thì b gọi là *ước thực sự* của a, kí hiệu là $b \parallel a$.

Liên hệ giữa tính chất chia hết và ideal sinh bởi một phần tử ta có

Định lí 2. *Cho X là miền nguyên, a, $b \in X$ và $b \neq 0$. Khi đó*

1) $b \mid a \Leftrightarrow \langle b\rangle \supset \langle a\rangle$.

2) $b \parallel a \Leftrightarrow \langle b\rangle \underset{\neq}{\supset} \langle a\rangle$.

CHỨNG MINH. 1) $b \mid a \Leftrightarrow \exists x \in X, a = bx \Leftrightarrow a \in \langle b\rangle \Leftrightarrow \langle a\rangle \subset \langle b\rangle$.

2) $b \parallel a \Leftrightarrow \exists x \in X$, x không khả nghịch, không liên kết với a, $a = bx \Leftrightarrow a \in \langle b\rangle, b \notin \langle a\rangle \Leftrightarrow \langle a\rangle \underset{\neq}{\subset} \langle b\rangle$.

Cho miền nguyên X và $a, b \in X$. Phần tử $d \in X$ gọi là *ước chung lớn nhất* của a và b, kí hiệu là ƯCLN (a,b), nếu $d \mid a$, $d \mid b$ và với mọi $c \in X$, $c \mid a$, $c \mid b$ thì $c \mid d$.

Định lí 3. *Nếu d là ƯCLN (a, b) thì tập các ước chung lớn nhất của a và b trùng với tập các phần tử liên kết với d.*

CHỨNG MINH. Giả sử d' là một ước chung lớn nhất bất kì của a và b. Theo định nghĩa ta có $d' \mid d$ và $d \mid d'$. Vậy d' liên kết với d.

Bây giờ giả sử d' liên kết với d. Theo định lí 1 tồn tại u khả nghịch để $d = d'u \Leftrightarrow d' = du^{-1}$. Do đó $d \mid a$, $d \mid b$, $c \mid d$ thì cũng có $d' \mid a$, $d' \mid b$, $c \mid d'$. Vậy d' cũng là ước chung lớn nhất của a và b.

3. Phần tử nguyên tố và phần tử bất khả quy

Phần tử p của một miền nguyên X gọi là *nguyên tố* nếu $p \neq 0$, p không khả nghịch và với mọi $a, b \in X$, $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$.

Phần tử p gọi là *bất khả quy* nếu $p \neq 0$, p không khả nghịch và với mọi $a, b \in X$, $p = ab$ thì a khả nghịch hoặc b khả nghịch, nói cách khác là p *không có ước thực sự*.

Định lí 4. *Trong một miền nguyên X mọi phần tử nguyên tố đều là phần tử bất khả quy.*

CHỨNG MINH. Giả sử p là nguyên tố và a, b $\in$ X sao cho p = ab. Vì p | ab nên p|a hoặc p|b. Xét trường hợp p|a. Khi đó tồn tại u $\in$ X, a = pu. Từ đó p = p(ub), suy ra ub = 1. Vậy b là khả nghịch.

§2. VÀNH CHÍNH

1. Định nghĩa vành chính

Một miền nguyên X gọi là một *vành chính* nếu mọi ideal của X đều là ideal chính.

Ví dụ 2. Mọi ideal của vành số nguyên $\mathbb{Z}$ đều có dạng $m\mathbb{Z} = \langle m \rangle$, do đó đều là ideal chính. Vậy $\mathbb{Z}$ là vành chính.

Định lí 5. *Trong vành chính X không tồn tại dãy vô hạn các phần tử $a_1, a_2, \ldots, a_n, \ldots$, trong đó a_{i+1} là ước thực sự của a_i với mọi i = 1, 2,..., n,..*

CHỨNG MINH. Nếu có một dãy như thế thì theo định lí 2 ta có dãy các ideal lồng nhau

$$\langle a_1 \rangle \underset{\neq}{\subset} \langle a_2 \rangle \underset{\neq}{\subset} \langle a_3 \rangle \underset{\neq}{\subset} \ldots$$

Dễ dàng kiểm tra $A = \bigcup_i \langle a_i \rangle$ là một ideal của X, do đó tồn tại a $\in$ X sao cho $\langle a \rangle = A$. Vì a $\in$ A nên $a \in \langle a_{i_0} \rangle$ với i_0 nào đó. Với $n > i_0$ theo định lí 2 ta có

$$\langle a_{i_0} \rangle \subset \langle a_n \rangle \subset \langle a_{n+1} \rangle \subset A \subset \langle a_{i_0} \rangle.$$

Vậy $\langle a_n \rangle = \langle a_{n+1} \rangle$ mà điều này mâu thuẫn với a_{n+1} là ước thực sự của a_n.

2. Vành nhân tử hóa

Cho X là một miền nguyên. Phần tử $a \in X$ gọi là *phân tích được một cách duy nhất thành tích các phần tử bất khả quy* nếu tồn tại các phần tử bất khả quy $p_1, p_2, ..., p_n$ sao cho $a = p_1.p_2...p_n$ và sự phân tích đó là duy nhất, nếu không kể đến thứ tự và các nhân tử khả nghịch. Nói cách khác, nếu cũng có $a = q_1.q_2...q_m$ với các q_i bất khả quy thì m = n và với một cách đánh số thích hợp ta có p_i liên kết với q_i với mọi i = 1, 2, ..., n.

Miền nguyên được gọi là *vành nhân tử hóa* hay *vành Gauss* nếu mọi phần tử khác không, không khả nghịch của nó đều phân tích được một cách duy nhất thành tích của các phần tử bất khả quy.

Định lí 6. *Mọi vành chính đều là vành nhân tử hóa.*

CHỨNG MINH. Giả sử a là một phần tử khác không, không khả nghịch của vành chính X. Trước hết ta chứng minh a có một ước bất khả quy. Thật vậy, nếu trái lại a không có ước bất khả quy nào thì a không bất khả quy và có một ước thực sự a_1 cũng không bất khả quy, a_1 lại có một ước thực sự không bất khả quy a_2, ... Ta được dãy a_1, a_2, ... vô hạn các phần tử mà phần tử đứng sau là ước thực sự của phần tử đứng liền trước, theo định lí 5 là một điều mâu thuẫn.

Giả sử p_1 là một ước bất khả quy của a. Khi đó $a = p_1a_1$. Nếu a_1 không bất khả quy thì tồn tại ước bất khả quy p_2, $a_1 = p_2a_2$, $a = p_1p_2.a_2$, ... Theo định lí 5, sau n bước ta sẽ có a_n bất khả quy, đặt $p_n = a_n$ ta được $a = p_1p_2...p_n$ là tích của các phần tử bất khả quy.

Bây giờ giả sử a có hai cách phân tích thành tích của các phần tử bất khả quy

$$a = p_1p_2 \dots p_n = q_1q_2 \dots q_m .$$

Ta có thể giả thiết $n \le m$. Vì mọi phần tử bất khả quy đều nguyên tố và $p_i \mid q_1q_2 \dots q_m$ nên tồn tại q_j sao cho $p_i \mid q_j$. Nếu cần thì đánh số lại, ta có thể giả thiết $p_i \mid q_i$. Vì p_i và q_i bất khả quy nên tồn tại phần tử u_i khả nghịch sao cho $q_i = p_i . u_i$. Từ đó

$$q_1 . q_2 \dots q_n = p_1 . p_2 \dots p_n . u = au$$

với $u = u_1u_2 \dots u_n$ là một phần tử khả nghịch. Nếu m > n thì

$$a = q_1q_2 \dots q_nq_{n+1} \dots q_m = au q_{n+1} \dots q_m$$

Suy ra $q_{n+1} \dots q_m = u^{-1}$ là một phần tử khả nghịch, ta gặp mâu thuẫn. Vậy m = n và $q_i = p_i u_i$ với mọi i = 1, 2, ..., n.

§3. VÀNH EUCLIDE

1. Định nghĩa vành Euclide

Cho X là một miền nguyên. Kí hiệu $X^* = X \setminus \{0\}$.

Miền nguyên X gọi là *vành Euclide* nếu có một ánh xạ

$$\delta : X^* \to \mathbb{N}$$

thỏa mãn các điều kiện

1) Nếu $b \mid a$ và $a \neq 0$ thì $\delta(b) \le \delta(a)$.

2) Với mọi $a, b \in X$, $b \neq 0$, tồn tại $q, r \in X$ sao cho $a = bq + r$ trong đó $r = 0$ hoặc $\delta(r) < \delta(b)$.

Ví dụ 3. Theo định lí phép chia có dư trong $\mathbb{Z}$, với ánh xạ

$$\delta : \mathbb{Z}^* \to \mathbb{N},$$
$$n \mapsto |n|$$

vành số nguyên $\mathbb{Z}$ là một vành Euclide.

Định lí 7. *Mọi vành Euclide đều là vành chính.*

CHỨNG MINH. Giả sử X cùng ánh xạ $\delta : X^* \to \mathbb{N}$ là vành Euclide, A là ideal tùy ý của X. Nếu $A = \{0\}$ thì A là ideal chính sinh bởi 0. Xét trường hợp $A \neq \{0\}$. Tập $\{\delta(a) \mid a \in A, a \neq 0\} \subset \mathbb{N}$ có số nhỏ nhất, do đó có $a \in A$, $a \neq 0$ sao cho $\delta(a)$ là số nhỏ nhất nói trên.

Ta sẽ chứng minh $A = \langle a \rangle$. Thật vậy, với mọi $x \in A$ vì X là vành Euclide nên $x = aq + r$, trong đó $r = 0$ hoặc $\delta(r) < \delta(a)$. Nếu $r \neq 0$ thì $r = x - aq \in A$, $\delta(r) < \delta(a)$ mâu thuẫn với cách chọn phần tử a. Vậy $r = 0$ và $x = aq \in \langle a \rangle$. Từ đó $A = \langle a \rangle$ là ideal chính.

Nhận xét 1. Theo định lí 6 và 7 ta có : mọi vành Euclide đều là vành nhân tử hóa.

2. Thuật toán tìm ước chung lớn nhất

Tương tự như đối với số nguyên, có thể sử dụng thuật toán Euclide để tìm ước chung lớn nhất của hai phần tử trong vành Euclide.

Nhận xét 2. Dễ dàng thấy rằng

1) Nếu $a \mid b$ thì ƯCLN $(a, b) = a$.

2) Nếu $a = bq + r$, $b \neq 0$ thì ƯCLN (a, b) cũng là ƯCLN (b, r).

Giả sử $a, b \in X$, $b \neq 0$. Khi đó tồn tại q_0, $r_0 \in X$ sao cho

$$a = bq_0 + r_0,\ r_0 = 0 \text{ hoặc } \delta(r_0) < \delta(b).$$

Nếu $r_0 \neq 0$ thì ta có

$$b = r_0q_1 + r_1,\ r_1 = 0 \text{ hoặc } \delta(r_1) < \delta(r_0).$$

Nếu $r_1 \neq 0$ thì ta có

$$r_0 = r_1 q_2 + r_2, \; r_2 = 0 \text{ hoặc } \delta(r_2) < \delta(r_1)$$

. . . . . .

Vì $\delta(b) > \delta(r_0) > \delta(r_1) > \ldots$ nên sau một số hữu hạn bước ta phải có $r_{n+1} = 0$, tức là

$$r_{n-1} = r_n q_{n+1}.$$

Theo nhận xét 2. 1) ƯCLN $(r_n, r_{n-1}) = r_{n-1}$. Từ đó theo nhận xét 2. 2) ta có ƯCLN (a, b) = r_{n-1}.

§4. VÀNH ĐA THỨC

1. Định nghĩa vành đa thức

Cho A là một vành giao hoán có đơn vị. Ta gọi một đa thức trên A là một *tổng hình thức* có dạng

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

hay viết gọn lại là $f(x) = \sum_{k=0}^{n} a_k x^k$, trong đó

$a_0, a_1, \ldots, a_n \in A$ gọi là *các hệ tử*;

x là một kí hiệu được gọi là *ẩn* với quy ước

$$x^0 = 1, x^k = x.x\ldots x \text{ (k lần)}.$$

Nếu $a_n \neq 0$ thì a_n được gọi là *hệ tử cao nhất* của đa thức f(x), số n gọi là *bậc* của đa thức f(x), kí hiệu là deg f(x).

Hai đa thức f(x) và g(x) được gọi là *bằng nhau* nếu tất cả các hệ tử tương ứng của chúng đều bằng nhau, tức là nếu

$$f(x) = a_0 + a_1x + ... + a_nx^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + ... + b_mx^m, \quad b_m \neq 0$$

thì n = m và $a_i = b_i$, i = 0, 1, ..., n.

Với mọi c∈A ta gọi $f(c) = a_0 + a_1c + ... + a_nc^n \in A$ là *giá trị của đa thức* f(x) tại c.

Một đa thức dạng ax^k gọi là *một đơn thức*. Như vậy một đa thức là tổng của một số hữu hạn các đơn thức hay các số hạng. Ta không phân biệt thứ tự các số hạng của một đa thức. Đa thức

$$a_0 + a_1x + ... + a_nx^n$$

được gọi là *viết dưới dạng chính tắc tiến*, còn đa thức

$$a_nx^n + a_{n-1}x^{n-1} + ... + a_0$$

được gọi là *viết dưới dạng chính tắc lùi*.

Tập tất cả các đa thức của ẩn x trên vành A kí hiệu là A[x].

2. Phép toán đa thức

Cho hai đa thức trên vành A

$$f(x) = a_0 + a_1x + ... + a_nx^n,$$

$$g(x) = b_0 + b_1x + ... + b_mx^m.$$

Ta gọi tổng của f(x) và g(x) là đa thức

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m +$$

$$+ a_{m+1}x^{m+1} + ... + a_nx^n,$$ ở đây ta giả sử n ≥ m.

Ta gọi tích của f(x) và g(x) là đa thức

$$f(x).g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \dots +$$

$$+ (a_nb_{m-1} + a_{n-1}b_m)x^{n+m-1} + a_nb_mx^{n+m}.$$

Như vậy tổng của hai đa thức là đa thức có các hệ tử bằng tổng các hệ tử tương ứng của hai đa thức đó.

Tích của hai đa thức f(x) và g(x) viết gọn lại là

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_ix^i$$

trong đó $c_i = \sum_{j+k=i} a_jb_k$, $i = 0, 1, \dots, n + m$.

Ta có kết quả sau đây :

Định lí 8. *Với mọi vành giao hoán có đơn vị A, với phép toán cộng và nhân đa thức, A[x] là một vành giao hoán, có đơn vị.*

Phần tử 0 là đa thức có tất cả các hệ số bằng không.

Phần tử 1 là đa thức 1 chỉ có hệ số $a_0 = 1$ còn tất cả các hệ số khác bằng không.

Vành A[x] gọi là *vành đa thức* trên A.

Từ định nghĩa các phép toán ta có

Định lí 9. *Với mọi f(x), g(x) ∈ A[x] ta có*

1) deg (f(x) + g(x)) ≤ max $\{\deg f(x), \deg g(x)\}$*, nếu deg f(x) ≠ deg g(x) thì* $\deg(f(x) + g(x)) = \max\{\deg f(x), \deg g(x)\}$.

2) deg $(f(x).g(x))$ *≤ deg f(x) + deg g(x), nếu A là miền nguyên thì deg (f(x) g(x)) = deg f(x) + deg g(x).*

Nhận xét 3. Để định lí 9 đúng trong mọi trường hợp, cần định nghĩa $\deg 0 = -\infty$ và với mọi $n \in \mathbf{N}$, $-\infty + n = -\infty$ và $-\infty < n$. Từ 2) của định lí 9 đặc biệt suy ra : Nếu A là miền nguyên thì A[x] cũng là miền nguyên.

2. Phép chia có dư

Định lí 10. *Cho A là một miền nguyên, f(x), g(x) ∈ A[x] và g(x) có hệ tử cao nhất khả nghịch. Khi đó tồn tại duy nhất g(x), r(x) ∈ A[x] sao cho*

$$f(x) = g(x)\,q(x) + r(x)$$

trong đó r(x) = 0 hoặc deg r(x) < deg g(x).

Đa thức q(x) gọi là *thương*, đa thức r(x) gọi là *dư* của phép chia đa thức f(x) cho g(x).

CHỨNG MINH. *Tính duy nhất.* Giả sử q'(x), r'(x) ∈A[x] cũng có tính chất đòi hỏi. Khi đó

$$g(x)\,q(x) + r(x) = g(x)\,q'(x) + r'(x).$$

Từ đó $g(x)\big(q(x) - q'(x)\big) = r'(x) - r(x)$. Nếu $r'(x) - r(x) \neq 0$ thì theo định lí 9

$$\deg\big(r'(x) - r(x)\big) = \deg g(x) + \deg\big(q(x) - q'(x)\big) \geq \deg g(x).$$

Đây là một điều mâu thuẫn vì deg r(x) < deg g(x),
deg r'(x) < deg g(x). Vậy r'(x) − r(x) = 0. Do A[x] là miền nguyên nên cũng có q(x) − q'(x) = 0.

Sự tồn tại. Ta chứng minh bằng quy nạp theo bậc của f(x). Giả sử $g(x) = b_m x^m + \ldots + b_1 x + b_0$, b_m là phần tử khả nghịch. Nếu deg f(x) < m thì chọn q(x) = 0, r(x) = f(x), định lí đúng.

Giả sử kết quả đúng với mọi đa thức có bậc nhỏ hơn n, n ≥ m. Xét đa thức f(x) có bậc n bất kì

$$f(x) = a_n x^n + \ldots + a_1 x + a_0,\ a_n \neq 0.$$

Đặt $\bar{f}(x) = f(x) - a_n b_n^{-1} x^{n-m} . g(x)$. Ta có $\bar{f}(x) = 0$ hoặc $\deg \bar{f}(x) < n$. Theo giả thiết quy nạp tồn tại $\bar{q}(x)$ và $r(x) \in A[x]$ sao cho

$$\bar{f}(x) = g(x)\, \bar{q}(x) + r(x)$$

với $r(x) = 0$ hoặc $\deg r(x) < \deg g(x) = m$. Từ đó

$$f(x) = g(x) \left(\bar{q}(x) + a_n b_m^{-1} x^{n-m}\right) + r(x)$$

Đặt $q(x) = \bar{q}(x) + a_n b_m^{-1} x^{n-m}$, ta có cặp $q(x)$ và $r(x) \in A[x]$ để $f(x) = g(x)\, q(x) + r(x)$ thỏa mãn $r(x) = 0$ hoặc $\deg r(x) < \deg g(x)$.

Định lí 1. *Nếu F là một trường thì vành F[x] là vành Euclide và do đó là vành nhân tử hóa.*

CHỨNG MINH. Xét ánh xạ $\delta : F[x]^* \to \mathbb{N}$, $\delta(f(x)) = \deg f(x)$.

Nếu $g(x) \mid f(x)$ thì $f(x) = g(x)\, u(x)$, do đó

$$\deg f(x) = \deg g(x) + \deg u(x) \geq \deg g(x).$$

Vậy $\delta(f(x)) \geq \delta(g(x))$.

Với mọi $f(x), g(x) \in F[x]$, $g(x) \neq 0$ theo định lí 10 tồn tại $q(x)$, $r(x) \in F[x]$ sao cho

$$f(x) = g(x)\, q(x) + r(x),\ r(x) = 0 \text{ hoặc } \delta(r(x)) < \delta(g(x))$$

Vậy theo định nghĩa, F[x] là vành Euclide.

Nhận xét 4. Vì F[x] là vành Euclide nên ước chung lớn nhất của hai đa thức khác không bất kì trên trường F tồn tại và có thể được tính theo thuật toán Euclide (Xem §3).

Ví dụ 5. Tìm ước chung lớn nhất của hai đa thức

$$f(x) = x^5 + 2x^3 + x^2 + x + 1$$

và $g(x) = x^4 - x^3 + 2x^2 - x + 1$ trong $Q[x]$.

Theo thuật toán Euclide ta có

$$f(x) = g(x).q_0(x) + r_0(x),\ q_0(x) = x + 1,\ r_0(x) = x^3 + x$$

$$g(x) = r_0(x).q_1(x) + r_1(x),\ q_1(x) = x - 1,\ r_1(x) = x^2 + 1$$

$$r_0(x) = r_1(x).q_2(x),\ q_2(x) = x.$$

Vậy ƯCLN $(f(x), g(x)) = r_1(x) = x^2 + 1$.

4. Nghiệm của đa thức

Cho A là một miền nguyên và $f(x) \in A[x]$. Phần tử $c \in A$ gọi là một *nghiệm* của f(x) trong A nếu f(c) = 0.

Nếu B là một miền nguyên chứa A như một vành con thì cũng có thể coi $f(x) \in B[x]$. Khi đó f(x) có thể có nghiệm trong B nhưng không có nghiệm trong A.

Nếu $b \in B$ là nghiệm của một đa thức $f(x) \in A[x]$ thì b gọi là *phần tử đại số* trên A. Trong trường hợp trái lại ta gọi b là phần tử *siêu việt* trên A.

Một phần tử đại số (siêu việt) trên trường hữu tỉ $\mathbb{Q}$ được gọi vắn tắt là *phần tử đại số* (siêu việt).

Ví dụ 6. 2x – 1 có nghiệm trong $\mathbb{Q}$ nhưng không có nghiệm trong $\mathbb{Z}$; $\frac{1}{2} \notin \mathbb{Z}$ nhưng $\frac{1}{2}$ là phần tử đại số trên $\mathbb{Z}$.

Định lí 12. *(Bezout). Cho A là một miền nguyên. Khi đó phần tử $c \in A$ là nghiệm của đa thức $f(x) \in A[x]$ khi và chỉ khi f(x) chia hết cho x – c trong vành A[x].*

CHỨNG MINH. Theo định lí 10 ta có

$$f(x) = (x - c)q(x) + r(x)$$

trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg (x - c) = 1$. Do đó $r(x) = r \in A$. Vì vậy $f(c) = r$ và với mọi $x \in A$

$$f(x) = (x - c)\, q(x) + f(c)$$

Từ đẳng thức này suy ra $f(x) = (x - c)q(x) \Leftrightarrow f(c) = 0$.

Cho $f(x)$ là một đa thức trên miền nguyên A và c là một nghiệm của $f(x)$. Khi đó tồn tại $k \in N^*$ sao cho $f(x)$ chia hết cho $(x-c)^k$ nhưng không chia hết cho $(x-c)^{k+1}$. Nếu $k = 1$ thì c gọi là *nghiệm đơn*, $k = 2$ thì c gọi là *nghiệm kép*, $k \geq 3$ thì c gọi là *nghiệm bội*. Trong trường hợp chưa biết k bằng bao nhiêu thì ta gọi chung c là *nghiệm bội k*.

Định lí 13. *Cho F là một trường và $f(x) \in F[x]$, $f(x) \neq 0$, $c_1, c_2, \ldots, c_r$ là các nghiệm của $f(x)$ với số lần bội $k_1, k_2, \ldots, k_r$. Khi đó tồn tại $g(x) \in F[x]$ sao cho*

$$f(x) = (x - c_1)^{k_1}(x - c_2)^{k_2} \ldots (x - c_r)^{k_r} g(x)\,,\ g(c_i) \neq 0 \text{ với } i = 1, 2, \ldots, r.$$

CHỨNG MINH. Theo định lí 11, F[x] là vành nhân tử hóa. Vì $x - c_i$ là các phần tử bất khả quy nên trong sự phân tích $f(x)$ thành tích các phần tử bất khả quy, sai khác một phần tử khả nghịch, sẽ có k_i thừa số $x - c_i$, $i = 1, 2, \ldots, r$. Đặt $g(x)$ là tích của các thừa số còn lại, ta có

$$f(x) = (x - c_1)^{k_1}(x - c_2)^{k_2} \ldots (x - c_r)^{k_r} g(x),\ g(c_i) \neq 0,\ i = 1, 2, \ldots, r.$$

Định lí 14. *Cho $f(x)$ là một đa thức trên trường F, $f(x) \neq 0$. Khi đó số nghiệm của $f(x)$, mỗi nghiệm tính với số lần bội của nó, không vượt quá $\deg f(x)$.*

CHỨNG MINH. Giả sử $f(x)$ có r nghiệm khác nhau c_i với số lần bội k_i, $i = 1, 2, \ldots, r$. Theo định lí 13 ta có

$$f(x) = (x - c_1)^{k_1}(x - c_2)^{k_2} \ldots (x - c_r)^{k_r} g(x)$$

Suy ra $\qquad \deg f(x) = k_1 + k_2 + \ldots + k_r + \deg g(x)$

Vậy $k_1 + k_2 + \ldots + k_r \le \deg f(x)$.

Định lí 15. *Cho $f(x)$ và $g(x)$ là hai đa thức bậc n trên trường F và có $n + 1$ phần tử $c_1, c_2, \ldots, c_{n+1} \in F$, sao cho $f(c_i) = g(c_i)$, $i = 1, 2, \ldots, n + 1$. Khi đó $f(x) = g(x)$.*

CHỨNG MINH. Xét đa thức $h(x) = f(x) - g(x)$. Nếu $h(x) \neq 0$ thì $h(x)$ có $n + 1$ nghiệm trong khi $\deg h(x) \le n$, là một mâu thuẫn do định lí 14. Vậy $h(x) = 0$ và $f(x) = g(x)$.

5. Sơ đồ Horner

Cho $f(x)$ là một đa thức bậc n trên một miền nguyên A và $c \in A$. Theo định lí 12

$$f(x) = (x - c)q(x) + r \qquad (1),\ \deg q(x) = n - 1,\ r \in A.$$

Giả sử $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$,

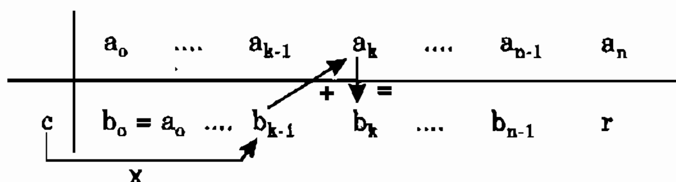
$$g(x) = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}.$$

Thay vào (1), thực hiện phép tính ở vế phải và so sánh hệ tử của hai vế, ta có

$$\begin{cases} a_0 = b_0 \\ a_1 = b_1 - cb_0 \\ \ldots\ldots \\ a_k = b_k - cb_{k-1} \\ \ldots\ldots\ldots \\ a_n = r - cb_{n-1} \end{cases} \Rightarrow \begin{cases} b_0 = a_0 \\ b_1 = cb_0 + a_1 \\ \ldots\ldots \\ b_k = cb_{k-1} + a_k \\ \ldots\ldots\ldots \\ r = cb_{n-1} + a_n \end{cases}$$

Từ đó ta dễ dàng tính được các hệ tử của $g(x)$ và r các hệ tử của $f(x)$ và c.

Dãy đẳng thức truy hồi đó được mô tả dưới dạng sơ đồ dưới đây, gọi là sơ đồ Horner :



Sơ đồ Horner cho ta thực hiện nhanh phép chia đa thức f(x) cho đa thức x – c. Vì f(c) = r nên nó cũng cho ta cách tính nhanh giá trị f(c).

Ví dụ 7. Tìm thương và dư của phép chia đa thức

$$f(x) = 2x^4 - x^3 + x^2 - 3x + 2 \text{ cho } x - 2.$$

Ta có sơ đồ Horner

	2	–1	1	–3	2
2	2	3	7	11	24

Từ đó thương là $2x^3 + 3x^2 + 7x + 11$, dư là 24 = f(2).

BÀI TẬP CHƯƠNG IV

4.1. Cho a, b là các phần tử của một vành chính X, ƯCLN (a, b) = d. Kí hiệu <a, b> là ideal của X sinh bởi tập hai phần tử a, b. Chứng minh rằng <a, b> = <d>.

4.2. Cho X là một vành chính và A là một ideal của X. Chứng minh rằng

a) Mọi ideal của vành X/A đều là ideal chính.

b) Vành X/A chính ⇔ ideal A nguyên tố.

4.3. Cho X là một vành chính. Chứng minh rằng

a) Nếu p là phần tử bất khả quy thì <p> là ideal tối đại.

b) Nếu P là ideal nguyên tố khác $\{0\}$ thì P là ideal tối đại.

c) Mọi phần tử a, b $\in$X đều có ước chung lớn nhất.

4.4. Cho X là vành Eclide và A là một ideal của X. Chứng minh rằng vành thương X/A là vành Euclide $\Leftrightarrow$ A là ideal nguyên tố của X.

4.5. a) Chứng minh rằng mọi trường đều là vành Euclide.

b) Cho A là vành Euclide. Chứng minh rằng A là trường $\Leftrightarrow$ δ: $A^* \to \mathbb{N}$ là ánh xạ hằng.

4.6. Tính số đa thức bậc n của $\mathbb{Z}_3[x]$.

4.7. Chứng minh rằng đa thức $\bar{1}.x^2 + \overline{14} \in \mathbb{Z}_{15}[x]$ có 4 nghiệm trong $\mathbb{Z}_{15}$.

4.8. Cho vành giao hoán có đơn vị A và I là một ideal của A. Chứng minh rằng

a) $I[x] = \{f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x] \mid \text{mọi } a_i \in I\}$ là ideal của A[x].

b) $A[x]/I[x] \cong (A/I)[x]$.

c) I nguyên tố trong A $\Leftrightarrow$ I[x] nguyên tố trong A[x].

4.9. Chứng minh rằng $A[x]/\langle x\rangle \cong A$. Từ đó suy ra nếu <x> nguyên tố thì A là miền nguyên, nếu <x> là tối đại thì A là một trường.

4.10. Cho A là một vành giao hoán, có đơn vị. Chứng minh rằng các điều kiện sau tương đương

1) A là trường.

2) A[x] là vành Euclide.

3) A[x] là vành chính.

4.11. Cho A là một miền nguyên. Hãy tìm trường các thương của vành A[x].

4.12. Chứng tỏ rằng các số sau đây là số đại số

a) $\sqrt{5} + \sqrt[4]{5}$ b) $i + \sqrt[3]{2}$

4.13. Tìm ước chung lớn nhất của các đa thức

a) $f(x) = x^4 + x^3 - 3x^2 - 4x - 1$; $g(x) = x^3 + x^2 - x - 1$.

b) $f(x) = x^5 + x^4 - x^3 - 2x - 1$; $g(x) = 3x^4 + 2x^3 + x^2 + 2x - 2$.

4.14. Dùng sơ đồ Horner, biểu diễn f(x) theo lũy thừa của x – c.

a) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$, $c = -1$.

b) $f(x) = x^5$, $c = 1$.

4.15. a) Tìm một đa thức f(x) bậc 3 sao cho

$$f(x) - f(x - 1) = x^2.$$

b) Lập công thức tính tổng $S_n = 1^2 + 2^2 + ... + n^2$.

4.16. Chứng minh rằng nếu $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ có nghiệm hữu tỉ thì có ít nhất một trong ba số a, b, c là chẵn.

HƯỚNG DẪN GIẢI BÀI TẬP

CHƯƠNG I. PHÉP TOÁN VÀ NỬA NHÓM

1.1. Không kết hợp, không giao hoán, 0 là phần tử trung hòa bên phải.

1.2. a) Kết hợp, giao hoán.

b) Kết hợp, giao hoán, 1 là phần tử trung hòa.

1.4. Giả sử a, b $\in$ S, $\forall$x, y $\in$ X ta có

$$\big((a*b)*x\big)*y=\big(a*(b*x)\big)*y=a*\big((b*x)*y\big)$$
$$=a*\big(b*(x*y)\big)=(a*b)(x*y)$$

Vậy $a*b \in S$.

1.5. a) $(\mathbb{R}, *)$ là vị nhóm giao hoán, 0 là phần tử trung hòa. Phần tử -1 không khả đối xứng.

b) $(\mathbb{N}, \oplus)$ là nửa nhóm giao hoán.

1.6. $(a*b)*c=a*(b*c)$ $\big(=|a||b|c\big)$; 1 là phần tử trung hòa bên trái.

$$a=1,\ b=-1 \text{ thì } a*b\neq b*a.$$

1.7. $\forall x \in X,\ x*x=x \Rightarrow x\leq x.$

$\forall x, y \in X,\ x\leq y$ và $y\leq x \Rightarrow x*y=y$ và $y*x=x \Rightarrow y=x.$

$\forall x, y, z \in X,\ x\leq y$ và $y\leq z \Rightarrow x*y=y,\ y*z=z$

$\Rightarrow x*(y*z)=y*z,\ y*z=z \Rightarrow x*z=z \Rightarrow x\leq z.$

1.8. a) Phần tử trung hòa là $\varnothing$, chỉ có $\varnothing$ có phần tử đối xứng là $\varnothing$.

b) Phần tử trung hòa là X, chỉ có X có phần tử đối xứng là X.

1.9. $(a * b) * c = a * (b * c)\ \left(= \min\{a + b + c, 1\}\right)$

Phần tử trung hòa là 0. Chỉ có 0 có phần tử đối xứng là chính nó.

1.10. Trước hết chứng minh bằng quy nạp $b^n.a = a.b^n$. Thật vậy, hiển nhiên đẳng thức đúng với n = 1. Nếu đẳng thức đúng với n – 1 thì $b^n.a = b.b^{n-1}.a = b.a.b^{n-1} = a.b.b^{n-1} = a.b^n$.

Hiển nhiên $(ab)^n = a^n b^n$ đúng với n = 1. Nếu điều này đúng với n – 1 thì $(ab)^n = (ab)^{n-1}ab = a^{n-1}b^{n-1}a.b = a^{n-1}ab^{n-1}b =$ $= a^n b^n$, tức là đúng với n.

1.11. a) f đơn ánh, $f \circ g = f \circ h \Rightarrow \forall x \in X$, $f(g(x)) = f(h(x)) \Rightarrow \forall x \in X$, $g(x) = h(x) \Rightarrow g = h$. Vậy f thỏa mãn luật giản ước trái. Nếu f không đơn ánh thì tồn tại $x_1, x_2 \in X, x_1 \neq x_2$, $f(x_1) = f(x_2)$. Chọn $g(x) = x_1$, $h(x) = x_2$ với mọi $x \in X$, ta có $f \circ g = f \circ h$ nhưng $g \neq h$.

b) f toàn ánh thì $f(X) = X$, $g \circ f = h \circ f \Rightarrow \forall x \in X$, $g(f(x)) = h(f(x))$ $\Rightarrow g(y) = h(y), \forall y \in X \Rightarrow g = h$. Vậy f thỏa mãn luật giản ước phải. Nếu f không toàn ánh thì tồn tại $x_0 \in X \setminus f(X)$. Chọn g và h sao cho $g(x) = h(x)$ với mọi $x \in f(X)$ và $g(x_0) \neq h(x_0)$. Khi đó $g \circ h = h \circ f$ nhưng $g \neq h$.

CHƯƠNG II. NHÓM

2.1. $(m \oplus n) \oplus p = (m + n - 1) \oplus p = (m + n - 1) + p - 1$

$= m + (n + p - 1) - 1 = m + (n \oplus p) - 1$

$= m \oplus (n \oplus p)$

$m \oplus n = m + n - 1 = n + m - 1 = n \oplus m$

$m \oplus 1 = m + 1 - 1 = m$. Vậy 1 là phần tử trung hòa

$m \oplus (2 - m) = m + (2 - m) - 1 = 1$. Vậy $2 - m$ là phần tử đối xứng của m.

2.2. $x * e = x$ với $\forall x \Leftrightarrow x + e - 2xe = x \Leftrightarrow e(1 - 2x) = 0$ với $\forall x$ $\Leftrightarrow e = 0$. Vậy 0 là phần tử trung hòa.

Mọi $x \in \mathbb{R} \setminus \left\{\frac{1}{2}\right\}$, $x*x' = 0 \Leftrightarrow x + x' - 2xx' = 0 \Leftrightarrow x' = \frac{x}{2x-1}$

vì $x \neq \frac{1}{2}$. Vậy phần tử đối xứng của x là $\frac{x}{2x-1}$.

2.3. • Tìm phần tử trung hòa : $(a, b) * (x, y) = (a, b)$ với $\forall(a, b)$

$\Rightarrow (ax, bx + y) = (a, b) \Rightarrow \begin{cases} ax = a \\ bx + y = b \end{cases} \Rightarrow \begin{cases} x = 1 \\ y = 0 \end{cases}$

Thử lại ta thấy (1,0) là phần tử trung hòa.

• Tìm phần tử đối xứng của (a, b) :

$(a, b) * (a', b') = (1, 0) \Leftrightarrow (aa', ba' + b') = (1, 0)$

$\Rightarrow aa' = 1,\ ba' + b' = 0 \Rightarrow a' = \frac{1}{a},\ b' = -\frac{b}{a}$. Thử lại ta thấy $\left(\frac{1}{a}, -\frac{b}{a}\right)$ là phần tử đối xứng của $(a, b) \in X$.

$(2, 0) * (1,1) = (2, 1);\ (1,1) * (2,0) = (2,2) \Rightarrow$

$(2,0) * (1,1) \neq (1,1) * (2,0)$ nên phép toán $*$ không giao hoán.

2.4. Do $G \neq \emptyset$ nên tồn tại $b \in G$. Gọi e là nghiệm của phương trình $bx = b$, ta có $be = b$. Với mọi $a \in G$. Gọi c là nghiệm của phương trình $xb = a$ ta có $cb = a$. Khi đó

$$ae = (cb)e = c(be) = cb = a \Rightarrow ae = a \quad (1).$$

Gọi a' là nghiệm của phương trình $ax = e \Rightarrow aa' = e$ (2).

Gọi a" là nghiệm của phương trình $a'x = e \Rightarrow a'a'' = e$. Ta có

$$a'a = a'a\,e = (a'a)(a'a'') = a'(aa')a'' = a'ea'' = a'a''$$

$$\Rightarrow \quad aa' = e \quad (3).$$

$$ea = (aa')a = a(a'a) = a\,e \Rightarrow ea = a \quad (4).$$

Từ (1), (4), G có đơn vị là e. Từ (2), (3), mọi $a \in G$ có nghịch đảo là a'. Vậy G là nhóm.

2.5. a) $1_G \in G_n$. Mọi $x, y \in G_n$ ta có

$$(xy^{-1})^n = x^n(y^{-1})^n = x^n(y^n)^{-1} = 1_G \Rightarrow xy^{-1} \in G_n$$

b) $(m, n) = 1 \Rightarrow \exists u, v,\ mu + nv = 1$. Khi đó $\forall a \in G_m \cap G_n$,

$$a^m = 1_G, a^n = 1_G, a = a^{mu+nv} = (a^m)^u.(a^n)^v = 1_G.1_G = 1_G.$$

Vậy $G_m \cap G_n = \{1_G\}$.

2.6. a) Giả sử $G = \{a_1, a_2, ..., a_n\}$. Với mỗi a_i, ta có

$$a_iG = \{a_ia_1, a_ia_2, ..., a_ia_n\} = G,$$

Thật vậy, nếu trái lại thì tồn tại $j \neq k$ sao cho $a_ia_j = a_ia_k \Rightarrow a_j = a_k$ là một điều mâu thuẫn. Vậy phương trình $a_ix = a_j$ có nghiệm trong G với mọi $a_i, a_j \in G$. Tương tự, phương trình $ya_i = a_j$ cũng luôn có nghiệm trong G với mọi $a_i, a_j \in G$. Theo bài tập 2.4, G là một nhóm.

b) Một tập ổn định của một nửa nhóm với phép toán là một nửa nhóm con của nó. Do là phần tử của nhóm nên mọi phần tử của nó đều thỏa mãn luật giản ước. Vậy theo a) nó là một nhóm con của G.

2.7. Mọi x, y ∈ G ta có $xy = 1_G xy = (yx)^2 xy = yxyxxy = yxy1_G y =$

$= yxy^2 = yx1_G = yx$. Vậy G là nhóm Abel.

2.8. Giả sử a, b ∈ C(X). Ta sẽ chứng minh $ab^{-1} \in C(X)$. Thật vậy, với mọi x ∈ X ta có

$$ab^{-1}x = a\left(x^{-1}b\right)^{-1} = a\left(bx^{-1}\right)^{-1} = axb^{-1} = xab^{-1},$$

do đó $ab^{-1} \in C(X)$.

2.9. Với mọi x, y ∈ X ta có : $xy = 1_X \Leftrightarrow x = y^{-1} \Leftrightarrow yx = 1_X$. Từ đó

$(ab)^n \Leftrightarrow (ab.ab \ldots aba)\, b = 1_X$

$\Leftrightarrow b\,(ab\,.\,ab \ldots aba) = 1_X$

$\Leftrightarrow ba\,.\,ba \ldots ba = 1_X$

$\Leftrightarrow (ba)^n = 1_X$.

Suy ra cấp của ab bằng cấp của ba.

2.10. a) Vì [x] là nhóm con của G nên theo định lí Lagrange cấp của nhóm con [x] là ước của n, tức cấp của x là ước của n.

b) Giả sử x∈G, x có cấp k. Theo a) tồn tại $m \in \mathbf{N}^*$ để km = n.

Từ đó $x^n = \left(x^k\right)^m = 1_G^m = 1_G$.

2.11. Vì nhóm có cấp nguyên tố p nên trong nhóm tồn tại phần tử x khác phần tử đơn vị. Từ đó cấp của x lớn hơn 1 và là ước p

(theo bài 2.10). Do p nguyên tố nên cấp của x bằng p. Vậy nhóm là cyclic và x phần tử sinh.

2.12. a) Giả sử x là một phần tử sinh của nhóm G thì

$$G = \{x^n \mid n \in \mathbb{Z}\}.$$

Khi đó ta cũng có $G = \{(x^{-1})^n \mid n \in \mathbb{Z}\}$. Vì $x \neq x^{-1}$ nên G có hai phần tử sinh. Nếu x^{n_0} là một phần tử bất kì của G, $n_0 \neq \pm 1$. Khi đó $n_0 k \neq 1$ với mọi $k \in \mathbb{Z}$, do đó $x \notin [x^{n_0}]$, tức là x^{n_0} không phải là phần tử sinh của G.

b) Giả sử x là một phần tử sinh của nhóm G. Dễ thấy x^{-1} cũng là phần tử sinh của G. Vì G chỉ có một phần tử sinh nên $x = x^{-1} \Leftrightarrow x^2 = 1_G$. Vậy cấp của G không lớn hơn 2.

2.13. Giả sử nhóm G có hơn 1 phần tử. Lấy $x \in G$, $x \neq 1_G$. Vì G không có nhóm con không tầm thường và $[x] \neq \{1_G\}$ nên $[x] = G$. Vậy G là nhóm cyclic.

2.14. Theo bài tập 2.11, các nhóm cấp 2, 3, 5 là nhóm cyclic, do đó là nhóm Abel. Ta còn phải chứng minh mọi nhóm cấp 4 là nhóm Abel. Thật vậy, nếu trong nhóm có một phần tử cấp 4 thì nhóm là cyclic, do đó là nhóm Abel. Nếu trong nhóm không có phần tử cấp 4 nào thì mọi phần tử khác đơn vị đều có cấp 2, trường hợp này nhóm là nhóm Abel theo bài tập 2.7.

2.15. Nhóm S_3 không giao hoán, chẳng hạn a = (1, 3, 2), b = (2, 3, 1) có $a \circ b \neq b \circ a$. Do vậy S_3 không là nhóm cyclic. Vì S_3 cấp 6 nên nhóm con thực sự của nó có cấp 1, 2, 3 nên đều là nhóm cyclic.

2.16. Với mọi $a \in A$, $b \in B$ ta có

$$ab(ba)^{-1} = a(ba^{-1}b^{-1}) \in A \qquad (\text{vì } a \in A,\ ba^{-1}b^{-1} \in A)$$

$$ab(ba)^{-1} = (aba^{-1})b^{-1} \in B \qquad (\text{vì } aba^{-1} \in B, b^{-1} \in B)$$

Vậy $ab(ba)^{-1} \in A \cap B \Rightarrow ab(ba)^{-1} = 1_X \Rightarrow ab = ba$.

2.17. a) Mọi $x \in X$, $a \in [X, X]$ ta có

$$x^{-1}ax = a(a^{-1}x^{-1}ax) \in [X, X]$$

do đó $[X, X]$ là nhóm con chuẩn tắc.

Với mọi $x, y \in X$, $x^{-1}y^{-1}xy \in [X, X]$

$\Rightarrow xy[X, X] = yx[X, X]$. Vậy $X/_{[X,X]}$ là nhóm Abel.

b) $X/_A$ Abel $\Leftrightarrow \forall x, y \in X$, $xyA = yxA$

$$\Leftrightarrow \forall x, y \in X,\ x^{-1}y^{-1}xy \in A \Leftrightarrow [X,X] \subset A.$$

2.18. Giả sử $X/_A = [tA]$. Khi đó, mọi $x, y \in X$

$$xA = t^mA \Rightarrow x = t^ma_1, a_1 \in A$$

$$yA = t^nA \Rightarrow y = t^na_2, a_2 \in A.$$

Do $a_1, a_2 \in C(X)$ nên

$$xy = t^ma_1t^na_2 = t^{m+n}a_1a_2;$$

$$yx = t^na_2t^ma_1 = t^{n+m}a_2a_1 = t^{m+n}a_1a_2$$

Vậy $xy = yx$.

2.19. Dễ thấy $C(S)$ là nhóm con của nhóm $N(S)$. Mọi $x \in N(S)$, $a \in C(S)$ ta cần chứng minh $x^{-1}ax \in C(S)$. Với mọi $s \in S$, đặt $y = (x^{-1}ax)s(x^{-1}ax)^{-1}$, ta sẽ chứng minh $y = s$. Ta có

$y = x^{-1}axsx^{-1}a^{-1}x$. Do $x \in N(S)$ nên $xSx^{-1} = S$, tức là $\exists s' \in S$ để $xsx^{-1} = s' \Rightarrow y = x^{-1}as'a^{-1}x$. Do $a \in C(S)$ nên $as'a^{-1} = s'$ $\Rightarrow y = x^{-1}s'x$. Từ đó $y = x^{-1}(xsx^{-1})x = s$.

2.20. a) Thử trực tiếp các tiên đề của nhóm. Phần tử trung hòa là (0, 0, 0), phần tử đối xứng của (k_1, k_2, k_3) là

$$\left((-1)^{k_3+1}k_1, -k_2, -k_3\right).$$

b) $(1,0,0)^0 = (0, 0, 0)$. Với $n \geq 0$ nếu $(1,0,0)^n = (n, 0, 0)$ thì $(1,0,0)^{n+1} = (n, 0, 0)(1, 0, 0) = (n + 1, 0, 0)$. Do đó $(1,0,0)^n$ = $(n, 0, 0)$ với mọi $n \in \mathbb{N}$. Từ đó $(1,0,0)^{-n} = (n,0,0)^{-1} = (-n, 0, 0)$ với $n < 0$. Vậy $A = \{(k,0,0) \mid k \in \mathbb{Z}\}$.

Với mọi $x = (k_1, k_2, k_3) \in X$, $a = (k, 0, 0) \in A$ ta có

$$x^{-1}ax = \left((-1)^{k_3+1}k_1, -k_2, -k_3\right)(k, 0, 0)\left(k_1, k_2, k_3\right) = (\pm k, 0, 0) \in A$$

Vậy A là nhóm con chuẩn tắc của X.

2.21. Ánh xạ $f : \mathbb{Z} \to n\mathbb{Z}$, $f(k) = nk$ là đẳng cấu, do đó $\mathbb{Z} \cong n\mathbb{Z}$.

2.22. Cho $f : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ là một đồng cấu. Giả sử $f(1) = m$. Với mọi $k \in \mathbb{N}^*$: $k.f\left(\frac{1}{k}\right) = f\left(k.\frac{1}{k}\right) = f(1) = m \Rightarrow \frac{m}{k} = f\left(\frac{1}{k}\right) \in \mathbb{Z}$ $\Rightarrow m \,\vdots\, k$ với mọi $k \in \mathbb{N}^*$. Suy ra $m = 0$. Từ đó $f(1) = 0$. Với mọi $\frac{p}{q} \in \mathbb{Q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ ta có

$$q\,f\left(\frac{p}{q}\right) = f(p) = pf(1) = 0.$$

Vậy $f\left(\frac{p}{q}\right) = 0$ với mọi $\frac{p}{q} \in \mathbb{Q}$.

2.23. Nếu có một đẳng cấu $f : (\mathbb{R},+) \to (\mathbb{R}^*,.)$ thì tồn tại $x \in \mathbb{R}$ sao cho $f(x) = -1$. Khi đó ta gặp mâu thuẫn vì

$$-1 = f(x) = f\left(\frac{x}{2}+\frac{x}{2}\right) = f\left(\frac{x}{2}\right).f\left(\frac{x}{2}\right) > 0.$$

2.24. Giả sử $f : X \to X$, $f(x) = x^{-1}$. Dễ thấy f là một song ánh. Với mọi $x, y \in X$ ta có $f(xy) = (xy)^{-1} = y^{-1}x^{-1}$; $f(x)\,f(y) = x^{-1}y^{-1}$. Do đó f là đẳng cấu $\Leftrightarrow \forall x,y : y^{-1}x^{-1} = x^{-1}y^{-1} \Leftrightarrow$

$\left(y^{-1}x^{-1}\right)^{-1} = \left(x^{-1}y^{-1}\right)^{-1} \Leftrightarrow xy = yx \Leftrightarrow$ X là nhóm Abel.

2.25. a) Phần tử trung hòa là $\left(1_{G_1}, 1_{G_2}\right)$, phần tử đối xứng của $\left(x_1, x_2\right)$ là $\left(x_1^{-1}, x_2^{-1}\right)$.

b) Chọn $\left(x_1, x_2\right) \in G_1 \times G_2$, $G_1 = [x_1]$, $G_2 = [x_2]$. Dễ dàng thấy $\left(x_1, x_2\right)^{m.n} = \left(1_{G_1}, 1_{G_2}\right)$. Với mọi k sao cho $\left(x_1, x_2\right)^k = \left(1_{G_1}, 1_{G_2}\right)$ thì $x_1^k = 1_{G_1}$, $x_2^k = 1_{G_2}$, suy ra $k \,\vdots\, m$, $k \,\vdots\, n$. Vì $(m, n) = 1$ nên $k \,\vdots\, m.n$. Vậy $G_1 \times G_2$ là nhóm Cyclic với phần tử sinh là $\left(x_1, x_2\right)$.

Bây giờ giả sử $(m, n) = d > 1$. Khi đó gọi k là bội chung nhỏ nhất của m và n thì $k < m.n$. Với mọi $\left(x_1, x_2\right) \in G_1 \times G_2$ ta có $\left(x_1, x_2\right)^k = \left(1_{G_1}, 1_{G_2}\right)$, tức là mọi phần tử đều có cấp < cấp của nhóm. Vậy $G_1 \times G_2$ không là nhóm cyclic.

2.26. $(\mathbb{Z}, *)$ là một nhóm giao hoán, phần tử trung hòa là 2, phần tử đối xứng của m là 4 – m.

Nếu $m < n$ thì với mọi $p \in \mathbb{Z}$ ta có : $m + p - 2 < n + p - 2 \Rightarrow m * p < n * p$. Vậy $(\mathbb{Z}, *, \leq)$ là nhóm sắp thứ tự.

2.27. Giả sử $G = \{g_1, g_2, \dots, g_n\}$ với $g_1 < g_2 < \dots < g_n$. Trước hết ta chứng minh $g_1 = 1_G$. Thật vậy, nếu $g_1 \neq 1_G$ thì $g_1 < 1_G \Rightarrow g_1^2 < g_1$, mâu thuẫn với g_1 là phần tử nhỏ nhất. Từ đó ta cũng có

$$g_n < g_1 g_n < g_2 g_n < \dots < g_n^2 \Rightarrow g_n = 1_G,$$

ta gặp mâu thuẫn. Vậy G phải vô hạn.

2.28. b) $\overline{(a,b)} = \overline{(a'b')}, \overline{(c,d)} = \overline{(c',d')} \Rightarrow a + b' = b + a', c + d' = d + c'$

$$\Rightarrow (a + c) + (b' + d') = (b + d) + (a' + c')$$

$$\Rightarrow (a + c, b + d) \sim (a' + c', b' + d')$$

$$\Rightarrow \overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}.$$

Vậy quy tắc đã cho là phép toán trên $\overline{X}$.

Có thể kiểm tra tính chất kết hợp và giao hoán của phép toán trên X một cách dễ dàng.

Phần tử trung hòa : $\overline{(a,a)}$, $a \in X$.

Phần tử đối xứng của $\overline{(a,b)}$ là $\overline{(b,a)}$.

c) Với mọi $b, b' \in X$ ta có $a + b + b' = b + a + b'$

$$\Rightarrow (a + b, b) \sim (a + b', b') \Rightarrow \overline{(a + b, b)} = \overline{(a + b', b')}$$

Mọi $x, y \in X$, chọn tùy ý $b \in X$ ta có

$$j(x + y) = \overline{(x + y + b + b, b + b)}$$

$$= \overline{(x + b, b)} + \overline{(y + b, b)}$$

$$= j(x) + j(y)$$

Vậy j là đồng cấu.

Với mọi x, y $\in$ X, x $\neq$ y $\Rightarrow$ x + b + b $\neq$ b + y + b $\Rightarrow \overline{(x+b,b)} \neq \overline{(y+b,b)} \Rightarrow j(x) \neq j(y)$. Vậy j là đơn ánh và do đó là đơn cấu.

d) Giả sử $\overline{(a,b)} \in \overline{X}$, chọn tùy ý c $\in$ X. Ta có

$$\overline{(a,b)} = \overline{(a+c,c)} + \overline{(c,b+c)} = \overline{(a+c,c)} - \overline{(b+c,c)} \equiv a - b.$$

CHƯƠNG III. VÀNH VÀ TRƯỜNG

3.1. Ta có $(-x)^2 = (-x)(-x) = x^2$. Do đó $(-x)^{2k} = \left((-x)^2\right)^k = x^{2k}$.

3.2. $(-x)(-x^{-1}) = x.x^{-1} = 1_X, (-x^{-1})(-x) = 1_X$, do đó $-x$ khả nghịch và $(-x)^{-1} = -x^{-1}$.

3.3. Phần tử không là (0, 0); phần tử đối của (m, n) là (–m, –n); phần tử đơn vị là (1, 0).

3.4. Nếu X giao hoán thì với mọi f, g$\in X^S$, s $\in$ S ta có

$$(f.g)(s) = f(s) . g(s) = g(s).f(s) = (g.f)(s),$$

do đó f.g = g.f.

Nếu X có đơn vị thì hàm I, I(s) = 1_X với mọi s$\in$S là phần tử đơn vị của X^S.

3.5. $A = \{m + n\sqrt[3]{5} \mid m, n \in \mathbf{Z}\}$ không là vành con của $\mathbb{R}$.

Thật vậy $\sqrt[3]{5} \in A$ nhưng $\sqrt[3]{5} . \sqrt[3]{5} \notin A$.

3.6. Với mọi a, b $\in$ C(X), x $\in$ X ta có :

$(a - b)\,x = ax - bx = xa - xb = x\,(a - b) \Rightarrow a - b \in C(X)$;

$(ab)\,x = a(bx) = a(xb) = (ax)\,b = (xa)\,b = x(ab) \Rightarrow ab \in C(X)$.

3.7. a) Giả sử $a \in X$, a không phải là ước của không, n_a là cấp của a. Ta sẽ chứng minh $n_a = s$. Hiển nhiên $1 \le n_a \le s$. Với mọi $x \in X$ ta có

$$(n_a x)\,a = x(n_a a) = x.0_X = 0_X\,.$$

Vì a không là ước của không nên $n_a x = 0_X$ với mọi $x \in X$.

Suy ra $n_a \ge s$. Vậy $n_a = s$.

b) Nếu a có cấp hữu hạn thì tương tự a) ta có $n_a x = 0_X$ với mọi $x \in X$, mâu thuẫn với X có đặc số không.

c) Suy ra từ a).

3.8. Mọi $x \in X$, ta có $-x = (-x)^2 = x^2 = x \Rightarrow -x = x$.

Mọi $x, y \in X$, $(x + y)^2 = x + y \Rightarrow x^2 + xy + yx + y^2 = x + y$

$$\Rightarrow xy + yx = 0 \Rightarrow xy = -yx \Rightarrow xy = yx.$$

3.9. a) $a, b \in mX \Rightarrow a = ma', b = mb' \Rightarrow a - b = m\,(a' - b') \in mX$,

$a \in mX, x \in X \Rightarrow ax = ma'x \in mX, xa = xma' = mxa' \in mX$.

b) $a, b \in A \Rightarrow m(a - b) = ma - mb = 0 \Rightarrow a - b \in A$.

$a \in A, x \in X \Rightarrow m(ax) = (ma)\,x = 0x = 0, m(xa) = x(ma) = 0$

$\Rightarrow ax \in A, xa \in A$.

3.10. $x, y \in A + B \Rightarrow x = a_1 + b_1, y = a_2 + b_2, a_1, a_2 \in A, b_1, b_2 \in B$

$$\Rightarrow x - y = (a_1 - a_2) + (b_1 - b_2) \in A + B\,.$$

$z \in X$, $x = a_1 + b_1 \in A + B \Rightarrow z\,x = za_1 + zb_1 \in A + B$,

$xz = a_1 z + b_1 z \in A + B$.

3.11. a) Mọi $x + I_0, y + I_0 \in X/I_0$ ta có $xy + I_0 = yx + I_0$

vì $xy - yx = 0 \in I_0$.

b) X/I giao hoán $\Leftrightarrow \forall x, y \in X, xy - yx \in I \Leftrightarrow I_0 \subset I$.

3.12. Giả sử $f : \mathbb{Z} \to \mathbb{Z}$ là đồng cấu vành. Khi đó

$$f(1) = f(1.1) = f(1) f(1) \Rightarrow f(1) (f(1) - 1) = 0$$

$\Rightarrow$ $f(1) = 0$ hoặc $f(1) = 1$.

Nếu $f(1) = 0$ thì $f(n) = 0$ với mọi $n \in \mathbb{Z}$.

Nếu $f(1) = 1$ thì $f(n) = n$ với mọi $n \in \mathbb{Z}$.

Vậy chỉ có hai đồng cấu từ vành $\mathbb{Z}$ vào $\mathbb{Z}$ là đồng cấu không và đồng cấu đồng nhất.

3.13. b) Nếu $f(a + b\sqrt{7}) = a + b\sqrt{11}$ là đồng cấu thì

$f(7) = f(7 + 0\sqrt{7}) = 7 + 0\sqrt{11} = 7$

$f(7) = f\left((0 + \sqrt{7})(0 + \sqrt{7})\right) = f(0 + \sqrt{7}).f(0 + \sqrt{7}) = \sqrt{11}.\sqrt{11} = 11$,

ta gặp mâu thuẫn.

c) Nếu $f : \mathbb{Q}(\sqrt{7}) \to \mathbb{Q}(\sqrt{11})$ là đẳng cấu thì $f(1) = 1$. Từ đó suy ra $f(7) = 7$, $f(\sqrt{7}\sqrt{7}) = 7 \Rightarrow \left(f(\sqrt{7})\right)^2 = 7 \Rightarrow f(\sqrt{7}) = \sqrt{7}$.

Đây là một điều mâu thuẫn, vì $\sqrt{7} \notin \mathbb{Q}(\sqrt{11})$.

3.14. a) $\{0\}$ nguyên tố $\Leftrightarrow xy = 0$ thì $x = 0$ hoặc $y = 0$

$\Leftrightarrow$ X là miền nguyên.

b) $\{0\}$ tối đại $\Leftrightarrow$ mọi ideal A của X, $A \neq \{0\}$ thì $A = X$

$\Leftrightarrow$ X chỉ có hai ideal là $\{0\}$ và X

$\Leftrightarrow$ X là trường.

c) P nguyên tố $\Leftrightarrow$ $xy \in P$ thì $x \in P$ hoặc $y \in P$

$\Leftrightarrow (x + P).(y + P) = 0 + P$ thì $x + P = 0 + P$

hoặc $y + P = 0 + P$.

$\Leftrightarrow X/P$ là miền nguyên.

d) M tối đại $\Leftrightarrow X/M$ chỉ có hai ideal tầm thường là $\{0_{X/M}\}$ và X/M

$\Leftrightarrow X/M$ là trường

e) Suy ra từ c) và d) vì mọi trường là miền nguyên.

3.15. Ta chỉ cần chứng tỏ F(A) là một trường con.

Giả sử $a = xy^{-1} \in F(A), b = zt^{-1} \in F(A)$. Khi đó

$$a - b = (xt - zy)(yt)^{-1} \in F(A)$$

Nếu thêm $b \neq 0$ thì $z \neq 0$ do đó

$$ab^{-1} = xy^{-1}tz^{-1} = (xt)(yz)^{-1} \in F(A).$$

3.16. a) Phần tử không là $(0, 0_X)$, phần tử đối của (m, x) là $(-m, -x)$.

Phần tử đơn vị là $(1, 0)$.

b) $h(x + y) = (0, x + y) = (0, x) + (0, y) = h(x) + h(y)$;

$h(xy) = (0, xy) = (0, x)(0, y) = h(x)h(y)$,

Vậy h là đồng cấu. Rõ ràng $x \neq y \Rightarrow (0, x) \neq (0, y)$
$\Rightarrow h(x) \neq h(y)$ nên h là đơn cấu.

3.17. b) Phần tử không là $\frac{0}{x'}$, phần tử đối của $\frac{x}{x'}$ là $\frac{-x}{x'}$. Phần tử đơn vị là $\frac{1_A}{1_A} = \frac{x'}{x'}$, phần tử nghịch đảo của $\frac{x}{x'} \neq 0$ là $\frac{x'}{x}$.

c) $j(x+y) = \dfrac{x+y}{1_A} = \dfrac{x}{1_A} + \dfrac{y}{1_A} = j(x) + j(y)$

$j(xy) = \dfrac{xy}{1_A.1_A} = \dfrac{x}{1_A}.\dfrac{y}{1_A} = j(x).j(y)$,

vậy j là đồng cấu. Mặt khác $x \neq y$ thì $\dfrac{x}{1_A} \neq \dfrac{y}{1_A} \Rightarrow j(x) \neq j(y)$,

vậy j là đơn cấu.

d) Ta có $\dfrac{x}{x'} = \dfrac{x}{1_A}.\dfrac{1_A}{x'} = \dfrac{x}{1_A}.\left(\dfrac{x'}{1_A}\right)^{-1} = x.x'^{-1}$.

3.18. a) Phần tử không là $\begin{pmatrix} 0_F & 0_F \\ 0_F & 0_F \end{pmatrix}$, phần tử đối của $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ là

$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. Phần tử đơn vị là $\begin{pmatrix} 1_F & 0_F \\ 0_F & 1_F \end{pmatrix}$.

b) Thử trực tiếp.

c) Phần tử nghịch đảo của $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $ad - bc \neq 0$ là

$$\begin{pmatrix} d(ad-bc)^{-1} & -b(ad-bc)^{-1} \\ -c(ad-bc)^{-1} & a(ad-bc)^{-1} \end{pmatrix}$$

3.19. a) Với $z_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}$, $z_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$ ta có

$$z_1 - z_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ -(b_1 - b_2) & a_1 - a_2 \end{pmatrix} \in \mathbf{C}$$

$$z_1.z_2 = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -(a_1b_2 + b_1a_2) & a_1a_2 - b_1b_2 \end{pmatrix} \in \mathbf{C}$$

Mọi $z = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbf{C}$, $z \neq 0$, z có nghịch đảo là

$$z^{-1} = \begin{pmatrix} \dfrac{a}{a^2+b^2} & \dfrac{-b}{a^2+b^2} \\ \dfrac{b}{a^2+b^2} & \dfrac{a}{a^2+b^2} \end{pmatrix} \in \mathbf{C}.$$

b) $j(a_1 + a_2) = \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & a_1 + a_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix}$

$= j(a_1) + j(a_2)$.

$j(a_1a_2) = \begin{pmatrix} a_1a_2 & 0 \\ 0 & a_1a_2 \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix}$

$= j(a_1) . j(a_2)$

Tính đơn ánh là hiển nhiên.

c) Ta có $i^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$ và mọi $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbf{C}$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = a + ib.$$

3.20. a) $q_1 = \begin{pmatrix} a_1 & b_1 \\ -\overline{b_1} & \overline{a_1} \end{pmatrix}$, $q_2 = \begin{pmatrix} a_2 & b_2 \\ -\overline{b_2} & \overline{a_2} \end{pmatrix} \in 2$ thì

$$q_1 - q_2 = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ -\overline{b_1} + \overline{b_2} & \overline{a_1} - \overline{a_2} \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ -\overline{(b_1 - b_2)} & \overline{a_1 - a_2} \end{pmatrix} \in 2,$$

$$q_1q_2 = \begin{pmatrix} a_1a_2 - b_1\overline{b_2} & a_1b_2 + b_1\overline{a_2} \\ \overline{-b_1}\,a_2 - \overline{a_1}\,\overline{b_2} & \overline{-b_1}\,b_2 + \overline{a_1}\,\overline{a_2} \end{pmatrix}$$

$$= \begin{pmatrix} a_1a_2 - b_1\overline{b_2} & a_1b_2 + b_1\overline{a_2} \\ -\overline{(a_1b_2 + b_1\overline{a_2}} & \overline{a_1a_2 - b_1\overline{b_2}} \end{pmatrix} \in 2$$

Mọi $q = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in 2$, đặt $\alpha = a\overline{a} + b\overline{b}$.

$\alpha = 0 \Leftrightarrow a = b = 0$, do đó $q \neq 0$ thì $\alpha > 0$. Từ đó

$$q^{-1} = \begin{pmatrix} \dfrac{\overline{a}}{\alpha} & \dfrac{-b}{\alpha} \\ \dfrac{\overline{b}}{\alpha} & \dfrac{a}{\alpha} \end{pmatrix} \in 2.$$

c) Với mọi $q = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in 2$, đặt $a = a_1 + ia_2$, $b = b_1 + ib_2$,

$a_1, a_2, b_1, b_2 \in \mathbb{R}$, ta có

$$q = \begin{pmatrix} a_1 + i\,a_2 & b_1 + ib_2 \\ -b_1 + ib_2 & a_1 - ia_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} + \begin{pmatrix} i\,a_2 & 0 \\ 0 & -ia_2 \end{pmatrix} + \begin{pmatrix} 0 & b_1 \\ -b_1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & ib_2 \\ ib_2 & 0 \end{pmatrix}$$

$$= a_1 + a_2I + b_1J + b_2K.$$

3.21. a) Nếu trái lại $1 < 0$ thì $0 < -1 \Rightarrow 0.(-1) < (-1)(-1) \Rightarrow 0 < 1$, ta gặp mâu thuẫn. Vậy $0 < 1$.

b) Nếu $0 < a$ nhưng $a^{-1} < 0$ thì $a^{-1}.a < 0.a \Rightarrow 1 < 0$, ta gặp mâu thuẫn. Vậy $0 < a \Rightarrow 0 < a^{-1}$, $0 < a^{-1} \Rightarrow 0 < (a^{-1})^{-1} = a$.

c) Theo b) $a^{-1} < 0, b^{-1} < 0 \Rightarrow a^{-1}b^{-1} > 0$. Từ đó

$$a < b < 0 \Leftrightarrow a.a^{-1}b^{-1} < ba^{-1}b^{-1} < 0.a^{-1}b^{-1}$$

$$\Leftrightarrow b^{-1} < a^{-1} < 0.$$

d) $a < b \Rightarrow a + a < a + b < b + b$

$$\Rightarrow a.1 + a.1 < a + b < b.1 + b.1$$

$$\Rightarrow a(1 + 1) < a + b < b(1 + 1)$$

Vì $1 + 1 > 0$ nên $(1+1)^{-1} > 0$. Từ đó

$$\Rightarrow a < (a + b)(1+1)^{-1} < b$$

Vậy có $x_1 = (a+b)(1+1)^{-1}$ để $a < x_1 < b$

Tương tự ta lại tìm được $x_2, a < x_2 < x_1$, ... Ta tìm được vô số x thỏa mãn $a < x < b$.

3.22. Nếu có một thứ tự $\leq$ để biến trường số phức $\mathbb{C}$ thành một trường sắp thứ tự thì $0 < i^2 \Rightarrow 0 < -1$. Ta gặp mâu thuẫn.

CHƯƠNG IV. MỘT VÀI LỚP VÀNH ĐẶC BIỆT

4.1. Vì X là vành chính nên tồn tại $c \in X$, $\langle a, b \rangle = \langle c \rangle$. Ta sẽ chỉ ra c và d liên kết. Ta có $a, b \in \langle c \rangle$ nên $c|a, c|b \Rightarrow c|d$. Mặt khác, $c \in \langle a,b \rangle$ nên tồn tại $x, y \in X$, $c = ax + by$, $d|a, d|b \Rightarrow d|c$.

4.2. a) Xét $p : X \to X/A$ là toàn cấu chính tắc. Với mọi ideal B của X/A, $p^{-1}(B)$ là ideal của X. Do X là vành chính nên $p^{-1}(B) = \langle b \rangle$. Từ đó $B = \langle b + A \rangle$.

b) Vành $X/_A$ có mọi ideal đều là ideal chính. Do đó $X/_A$ là vành chính $\Leftrightarrow$ $X/_A$ là miền nguyên $\Leftrightarrow$ A là nguyên tố.

4.3. a) Giả sử A là một ideal chứa $<p>$. Khi đó $A = <a>$. Suy ra $p \in <a>$ $\Rightarrow$ $p = ab$. Vì p bất khả quy nên $a | 1$ hoặc $b | 1$. Khi đó $A = X$ hoặc $A = <p>$. Vậy $<p>$ là ideal tối đại.

b) Giả sử $P = <p>$. Nếu $p | ab$ thì $ab \in P$ do đó $a \in P$ hoặc $b \in P$ tức là $p | a$ hoặc $p | b$. Vậy p là phần tử nguyên tố, từ đó p là phần tử chính quy. Theo a) P là tối đại.

c) Tập $D = \{ax + by \mid x, y \in X\}$ là một ideal của X, do đó $D = <d>$. Vì $a = a.1 + b.0 \in D$, $b = a.0 + b.1 \in D$ nên $d | a$, $d | b$. Do $d \in D$ nên $d = as + bt$, $s, t \in X$. Nếu c có $c | a$, $c | b$ thì $c | as + bt \Rightarrow c | d$.

4.4. Nếu $X/_A$ là vành Euclide thì $X/_A$ là miền nguyên, do đó A là ideal nguyên tố. Ngược lại nếu A là ideal nguyên tố trong X thì hoặc $A = \{0\}$, hoặc A là ideal tối đại (Bài tập 4.3 b)). Khi đó $X/_A \cong X$ hoặc $X/_A$ là một trường. Vậy $X/_A$ là vành Euclide.

4.5. a) Giả sử F là một trường. Khi đó $\delta : F^* \to \mathbb{N}$, $\delta(x) = 1$ với mọi $x \in F^*$ là ánh xạ biến F thành vành Euclide.

b) Nếu A là trường thì mọi $x \in A^*$ ta có $1 = x.x^{-1}$, $x = 1.x \Rightarrow$ $\delta(x) \leq 1$ và $\delta(x) \geq 1 \Rightarrow \delta(x) = 1$.

Ngược lại, nếu δ là ánh xạ hằng thì với $x = 1$ và $y \neq 0$, tồn tại $q, r \in A$ sao cho $1 = yq + r$. Nếu $r \neq 0$ thì $\delta(r) < \delta(y)$ mâu thuẫn với δ là ánh xạ hằng, do đó $r = 0$. Vậy mọi $y \neq 0$ đều có nghịch đảo, A là một trường.

4.6. Giả sử đa thức có dạng

$$a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

Vì $a_0 \neq 0$ nên chọn a_0 có 2 cách. Chọn a_i, $i \neq 0$ có 3 cách. Do vậy theo quy tắc nhân ta có 2.3^n đa thức bậc n trong $\mathbb{Z}_3[x]$.

4.7. Bằng thử trực tiếp ta thấy $\bar{1}x^2 + \overline{14}$ có đúng 4 nghiệm trong $\mathbb{Z}_{15}$ là $\bar{1}, \bar{4}, \overline{11}, \overline{14}$.

4.8. a) Dễ thấy hiệu hai đa thức thuộc I[x] là một đa thức thuộc I[x]. Giả sử $f(x) \in I[x]$, $\deg f(x) = n$, $g(x) \in A[x]$, $\deg g(x) = m$. Khi đó $f(x)\, g(x) = c_0 x^{n+m} + c_1 x^{n+m-1} + \dots + c_{n+m}$,

trong đó mỗi c_i là tổng của các tích của hai phần tử, có ít nhất một phần tử thuộc I. Do I là ideal nên mọi tích này đều thuộc I. Từ đó $c_i \in I$ với $i = 0, 1, \dots, n + m$, tức là $f(x)\, g(x) \in I[x]$.

b) Xét ánh xạ $\varphi : A[x] \to \left(A/I\right)[x]$, với mọi

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ đặt } \varphi(f(x)) = \sum_{i=1}^{n} \overline{a_i} x^i,$$

trong đó $\overline{a_i} = a_i + I \in A/I$. Dễ kiểm tra φ là một toàn cấu vành. Mặt khác

$$\ker \varphi = \left\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid \sum_{i=0}^{n} \overline{a_i}\, x^i = \bar{0} \right\}$$

$$= \left\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid \overline{a_i} = \bar{0} \text{ với } i = 0, 1, \dots, n \right\}$$

$$= \left\{ f(x) = \sum_{i=0}^{n} a_i x^i \in A[x] \mid a_i \in I \text{ với } i = 0, 1, \dots, n \right\} = I[x].$$

Do đó theo định lí đồng cấu vành $A[x]/I[x] = A[x]/\ker\varphi \cong \left(A/I\right)[x]$

c) I nguyên tố trong A $\Leftrightarrow$ A/I là miền nguyên $\Leftrightarrow$ $(A/I)[x]$ là miền nguyên $\Leftrightarrow$ $A[x]/I[x]$ là miền nguyên $\Leftrightarrow$ I[x] nguyên tố.

4.9. Xét ánh xạ $\varphi : A[x] \to A$, $f(x) = a_0 + a_1x + \dots + a_nx^n \mapsto a_0$. Khi đó φ là một toàn cấu vành và

$$\ker \varphi = \{f(x) \in A[x] \mid f(x) \vdots x\} = <x>.$$

Vì vậy $A[x]/<x> \cong A$.

4.10. Chỉ cần chứng minh 3) ⇒ 1), tức là cần chứng minh nếu A[x] là vành chính thì mọi $x \in A$, $x \neq 0$ đều có nghịch đảo. Xét ideal <a, x> của A[x] sinh bởi hai phần tử a và x. Do A[x] là vành chính nên <a, x> = <d> với $d \in A$. Vì $d \mid x$ và $d \mid a$ nên d khả nghịch. Từ đó <a, x> = A[x]. Do $1 \in$ <a, x> nên tồn tại $f(x), g(x) \in A[x]$ sao cho $1 = af(x) + xg(x)$.

Với x = 0 ta có af(0) = 1. Vậy a khả nghịch.

4.11. Vì A là miền nguyên nên A[x] là miền nguyên, do đó A[x] có trường các thương xây dựng theo bài tập 3.17. Các phần tử của F(A[x]) có dạng $\frac{f(x)}{g(x)}$, $f(x) \in A[x]$, $g(x) \in A[x] \setminus \{0\}$. Phép toán trên F(A[x]) xác định bởi

$$\frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)g_2(x) + g_1(x)f_2(x)}{g_1(x)g_2(x)}$$

$$\frac{f_1(x)}{g_1(x)} \cdot \frac{f_2(x)}{g_2(x)} = \frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}$$

F(A[x]) là tập các phân thức hữu tỉ trên vành A. Vậy nếu A là một miền nguyên thì các phân thức hữu tỉ trên A tạo thành một trường với các phép toán như trên.

4.12. a) $\alpha = \sqrt{5} + \sqrt[4]{5} \Rightarrow \alpha - \sqrt{5} = \sqrt[4]{5} \Rightarrow \alpha^2 - 2\sqrt{5}\alpha + 5 = \sqrt{5}$

$\Rightarrow \alpha^2 + 5 = \sqrt{5}(2\alpha + 1) \Rightarrow (\alpha^2 + 5)^2 = 5(2\alpha + 1)^2$

$\Rightarrow \alpha^4 - 10\alpha^2 - 20\alpha + 20 = 0$.

Vậy α là nghiệm của đa thức $x^4 - 10x^2 - 20x + 20 \in \mathbb{Z}[x]$.

b) $\alpha = i + \sqrt[3]{2} \Rightarrow (\alpha - i)^3 = 2 \Rightarrow (\alpha^3 - 3\alpha - 2) - i(3\alpha^2 - 1) = 0$

$\Rightarrow [(\alpha^3 - 3\alpha - 2) - i(3\alpha^2 + 1)][(\alpha^3 - 3\alpha - 2) + i(3\alpha^2 + 1)] = 0$

$\Rightarrow (\alpha^3 - 3\alpha - 2)^2 + (3\alpha^2 + 1)^2 = 0$

$\Rightarrow \alpha^6 + 3\alpha^4 - 4\alpha^3 + 3\alpha^2 + 12\alpha + 5 = 0$

Vậy α là nghiệm của phương trình

$$x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5 = 0.$$

4.13. a) $x + 1$; b) $x^2 + 1$.

4.14. a) Theo sơ đồ Horner

	1	2	–3	–4	1
–1	1	1	–4	0	(1)
–1	1	0	–4	(4)	
–1	1	–1	(–3)		
–1	1	(–2)			

Từ sơ đồ trên ta có

$x^4 + 2x^3 - 3x^2 - 4x + 1 =$

$$= (x+1)^4 - 2(x+1)^3 - 3(x+1)^2 + 4(x+1) + 1$$

b) $(x-1)^5 + 5(x-1)^4 + 10(x-1)^3 + 10(x-1)^2 + 5(x-1) + 1$.

4.15. a) $f(x) = ax^3 + bx^2 + cx + d$

$f(x-1) = a(x-1)^3 + b(x-1)^2 + c(x-1) + d$

$= ax^3 + (-3a+b)x^2 + (3a-2b+c)x + (-a+b-c+d)$

$f(x) - f(x-1) = x^2$ khi

$$\begin{cases} 3a = 1 \\ -3a + 2b = 0 \\ a - b + c = 0 \end{cases} \Rightarrow \begin{cases} a = \dfrac{1}{3} \\ b = \dfrac{1}{2} \\ c = \dfrac{1}{6} \end{cases}, \text{ d tùy ý.}$$

Vậy $f(x) = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x + d.$

b) Theo a) ta có $1^2 = f(1) - f(0)$

$2^2 = f(2) - f(1)$

....

$n^2 = f(n) - f(n-1).$

Cộng các đẳng thức này, ta được

$$S_n = f(n) - f(0) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+1)(2n+1)}{6}.$$

4.16. Giả sử x_1 là một nghiệm hữu tỉ của f(x), khi đó

$$ax_1^2 + bx_1 + c = 0 \Rightarrow (ax_1)^2 + b(ax_1) + ac = 0.$$

Đặt $y_1 = ax_1$ thì y_1 là nghiệm hữu tỉ của phương trình

$$y^2 + by + ac = 0,$$

do đó y_1 là số nguyên. Gọi y_2 là nghiệm thứ hai của phương trình này thì y_2 cũng nguyên. Ta có $y_1 + y_2 = -b$, $y_1.y_2 = ac$, do đó $abc = -y_1y_2(y_1 + y_2)$. Vì trong 3 số nguyên y_1, y_2, $y_1 + y_2$ có ít nhất một số chẵn nên abc chẵn. Từ đó trong 3 số a, b, c có ít nhất một số chẵn.

MỤC LỤC

Chịu trách nhiệm xuất bản :
Chủ tịch HĐQT kiêm Tổng Giám đốc NGÔ TRẦN ÁI
Phó Tổng Giám đốc kiêm Tổng biên tập NGUYỄN QUÝ THAO

Tổ chức bản thảo và chịu trách nhiệm nội dung :
Phó tổng Giám đốc kiêm Giám đốc NXBGD tại TP. Hồ Chí Minh
VŨ BÁ HOÀ

Biên tập nội dung :
ĐẶNG THỊ BÌNH

Biên tập kĩ thuật:
TRẦN THÀNH TOÀN

Trình bày bìa :
VÕ THANH HÙNG

Sửa bản in:
HOÀNG KIM

Chế bản tại :
PHÒNG SCĐT – CN.NXBGD – TP. HỒ CHÍ MINH

CẤU TRÚC ĐẠI SỐ

Mã số : 7K580m9 – DAI

In 1.000 cuốn (QĐ: 08), khổ 14,5 x 20,5 cm. In tại Công ty Cổ phần In Phúc Yên.
Địa chỉ : Đường Trần Phú, thị xã Phúc Yên, Vĩnh Phúc.
Số ĐKKH xuất bản : 04 – 2009/CXB/399 – 2117/GD.
In xong và nộp lưu chiểu tháng 2 năm 2009.

TÌM ĐỌC SÁCH THAM KHẢO BỘ MÔN TOÁN BẬC TIỂU HỌC CỦA NHÀ XUẤT BẢN GIÁO DỤC

100 câu hỏi và đáp về việc dạy toán ở Tiểu học	*Phạm Đình Thực*
Dạy toán ở Tiểu học bằng phiếu giao việc	*Phạm Đình Thực*
Giảng dạy các yếu tố hình học ở Tiểu học	*Phạm Đình Thực*
Giải bài toán ở Tiểu học như thế nào ?	*Phạm Đình Thực*
Một số vấn đề suy luận trong môn toán ở Tiểu học	*Phạm Đình Thực*
Phương pháp sáng tác đề toán ở Tiểu học	*Phạm Đình Thực*
Toán chọn lọc Tiểu học	*Phạm Đình Thực*
Dạy học các tập hợp số ở bậc Tiểu học	*Nguyễn Phụ Hy (cb)*
Dạy học phép đo đại lượng ở bậc Tiểu học	*Nguyễn Phụ Hy (cb)*
Số học	*Đậu Thế Cấp*

Bạn đọc có thể mua sách tại các Công ti Sách – Thiết bị trường học ở các địa phương hoặc các cửa hàng sách của Nhà xuất bản Giáo dục :

– **Tại TP. Hà Nội** : 187 Giảng Võ ; 232 Tây Sơn ,
23 Tràng Tiền ; 25 Hàn Thuyên.
– **Tại TP. Đà Nẵng** : 15 và 62 Nguyễn Chí Thanh.
Tại TP.Hồ Chí Minh : 104 Mai Thị Lựu, Quận 1 ;
451 B - 453, Hai Bà Trưng, Quận 3 ;
240 Trần Bình Trọng, Quận 5.
Tại TP. Cần Thơ 5/5, đường 30/4.

Website : www.nxbgd.com.vn





Giá : 10.500 đ